McKeever CRMA Study System

John McKeever also authored McKeever CRMA Study System that sold over 1500 copies in 80 countries

Over 300 Practice Questions
Answers & Explanations

A CRMA Study System That Works!

CRMA Exam PASSED
Course Overview

Thank you for using the *McKeever CRMA Study System* as a tool to help you pass The IIA CRMA Exam.

Passing the exam portion of the CRMA exam involves 2 parts – 1) passing Part 1 of the CIA Exam and 2) passing the CRMA Exam.

The actual CRMA Exam questions are confidential. As a result, the material and practice questions presented are representative of the body of knowledge tested by the CRMA Exam. They are not actual questions from current or past CRMA Exams. The material has been developed and compiled to the best of the author’s knowledge and from applying CRMA principles as a Risk Management Practitioner.

The *McKeever CRMA Study System* will help you prepare for the CRMA Exam as follows:

1) describes the many areas covered by the CRMA Exam

2) presents over 300 practice questions similar to what you will see on the CRMA Exam

3) makes you comfortable with complexities and approaches required to choose the BEST answer

4) provides you with guidance for correct answers and feedback about incorrect answers

5) helps you identify areas on the CRMA Exam that will require your additional study time

The IIA web site lists a variety of study material and references to use in passing Part 1 of the CIA Exam. The IIA web site also contains a listing of reference to use for CRMA Exam.

The *McKeever CRMA Study System* covers the CRMA Exam in-depth.

The wording of multiple-choice questions can often be a greater challenge than the actual material being tested. Therefore, throughout this workbook there will be opportunities to understand both the technical material that may appear on the CRMA Exam as well as how to clarify the wording used in questions.
This material contains extensive discussion of the technical topics that may appear on the CRMA Exam. In addition, there are sample questions related to the topics. These modules contain the correct answer to each question along with an explanation, which examines the wording of the question. There are a substantial number of advanced questions. These questions are more typical of what will appear on the CRMA Exam. These advanced questions are presented in two parts. The first part provides the questions only. The second part is more comprehensive with the questions and their answers highlighted, along with an explanation of the correct answer. Periodically throughout the workbook, there will be extractions from these advanced questions to examine their wording content, keyword traps, and the technical content of the questions.

Although the discussions in each domain contain substantial material, it is advised that the participants review the advanced questions. Reviewing practice questions and becoming familiar with the wording of multiple-choice questions can be a great aid in the preparation for a multiple-choice format test.

There are also additional references available at www.pleier.com including the McKeever CCSA Study system, Achieving Audit Excellence, Risk Management Risk Assessment, Exceeding Expectations for Internal Auditors, and Transition: Internal Audit to Internal Assurance.

Although review courses by themselves including the McKeever CRMA Study System are generally not sufficient to ensure exam success this study system will certainly provide you with an approach to significantly improve your chances of passing. The IIA web site offers a variety of additional references for further study that is also listed in the Reference Module of this workbook.

Please feel free to contact me at johncbc@att.net.

Wishing You the Best of Success on the CCSA Exam,

John J. McKeever
CRMA, CCSA, CFE, CQA, CBM
John McKeever, President & COO of Contemporary Business Concepts, LLC., is probably best known as the author of the *McKeever CCSA Study System* and *McKeever CCSA Practice Test* used by 100s to pass the IIA CCSA Exam.

John frequently speaks at public seminars; professional associations; state and federal agencies; and corporations. His work includes developing and delivering risk and control management programs specifically focused for the needs of Senior Executives, Boards of Directors, and Audit Committees.

John has served as Operations Manager, Consultant, Instructor, and member of ATT&T audit staff. During 15 years in the audit department at AT&T, he conducted and led a wide range of audits and consulting projects. These included audits and projects of finance, operations, and information technology.

While in private practice; at the AT&T School of Business; and at The Institute of Internal Auditors John has developed and delivered a number of programs which include, *Consulting: A Value Added Service The Tools and Techniques That Make It Work*, *COSO The Steps To Success, Help Your Client Succeed with Control Self-Assessment*, and *The McKeever CCSA Study System*. For his achievements as a seminar leader, The Institute of Internal Auditors has awarded John the designation of Distinguished Adjunct Faculty Member.

In addition John has authored numerous research papers that have addressed the concepts of process improvement in business, employee empowerment, and the management of effective teams. Using these tools, he has guided and encouraged thousands of domestic and international professionals to move toward process and business improvements.

John has degrees in Business Administration and Management from Northeastern University, a Master of Science Degree in Management from Stevens Institute of Technology, and a graduate level Certificate in Total Quality Management from the University of Phoenix. He is a Certified Quality Auditor, a Certified Fraud Examiner, a Certified Business Manager, a Certified Professional Consultant, and holds a Certification in Risk Management Assurance. In addition, John holds both a Control Self-Assessment Qualification and a Certification in Control Self-Assessment.

He is a member of the American Society for Quality, The Institute of Internal Auditors, The Association of Business Professionals in Business Management, and the Association of Certified Fraud Examiners.
Index

Course Overview

Domain I: Organizational governance related to risk management

Domain II: Principles of risk management processes

Domain III: Assurance role of the Internal Auditor (IA)

Domain IV: Consulting role of the Internal Auditor (IA)

Suggested Additional References

Appendices

Application Questions

Application Questions, Answers & Explanations
Overview

CRMA® and the McKeever CRMA Study System

Certificate in Risk Management Assurance (CRMA)

The Certificate in Risk Management Assurance® (CCSA®) is a specialty certification program offered by The Institute of Internal Auditors (The IIA). It is designed for internal auditors who develop specialized risk management assurance skills. Gaining the required knowledge of areas such as risk and control exposes internal auditors to the concepts that are vital in more effectively using risk management principles to help clients achieve their objectives.

Internal auditors at any experience level, in almost all positions, will benefit from this certification program.

Visit the IIA’s web site www.theiia.org. There you will find a number of valuable resources listed to help you pass both Part 1 of the CIA Exam and the CRMA Exam.

Be certain to review The IIA’s web site resources in detail as the information listed there tells what you need to know about the requirements for becoming a CRMA including professional experience and CRMA Exam overview.

The McKeever CRMA Study System builds on the information available at The IIA web site. It does not replace the need to review the information on that web site.

The McKeever CRMA Study System provides a studying methodology and techniques to help you successfully pass the CRMA Exam. In addition, you should find that the McKeever CRMA Study System is an excellent, practical, application reference source for applying risk management principles in practice.
McKeever CRMA Study System

The McKeever CRMA Study System provides the following to help you successfully pass the CRMA Exam:

1) outlines how to study for the CRMA Exam

2) explains, in detail, the information you need about the contents of each domain on the CRMA Exam and demonstrates techniques to address multiple-choice question

3) provides over 300 sample questions, with answers and explanations, similar to the ones you will see on the CRMA Exam - not the actual questions that may appear on the CRMA Exam since the actual exam questions are confidential

4) provides an extremely valuable resource for both self-study mode and group training

5) helps you identify areas where you need additional study prior to the exam

6) provides a guide for resources to use in preparing to pass the exam

How to Study for the CRMA Exam

There is no standard way to study for the CRMA Exam as each person has an individual study style. However, the McKeever CRMA Study System does provide proven test-taking techniques.

The McKeever CRMA Study System:

Study the modules covering CRM Domains in any sequence

Limit study to a comfortable time in both group study and self-study

Do not try to cover everything in one session

For group study we recommend no less than 16 hours of team study. This time should include reviews of both the content in the modules and review of the Sample Questions with Answers and Explanations.

While studying the material you will see a STOP sign with a sample question. Try to determine the “best answer”. Then look at the answer and explanation in the Application Questions, Answers & Explanation module.
Review the Application Questions module after studying the Domain modules.

DOMAIN I:
ORGANIZATIONAL GOVERNANCE RELATED TO RISK MANAGEMENT EXTRACT
Domain I: Organizations and Organizational Culture

The objective of this module is to better prepare the participant to pass the Certification in Risk Management Assurance Exam by discussing and analyzing the technical dimensions of this domain while discussing techniques to best manage multiple-choice questions.

Included are discussions of the skill requirements of a CRMA to:

A. Assess risk management processes in the context of alignment with strategic imperatives
   1) Objectives of risk management processes
   2) Organization’s risk culture
   3) Risk capacity, appetite, and tolerance of organization

B. Assess the processes related to the elements of the internal environment in which organizations seek to manage risks and achieve objectives
   1) Integrity, ethical values, and other soft controls
   2) Role, authority, responsibility, etc., for risk management
   3) Management’s philosophy and operating style
   4) Legal / Organizational structure
   5) Documentation of governance-related decision-making
   6) Capabilities, in terms of people and other resources (e.g., capital, time, processes, systems, and technologies)
   7) Management of third party business relationships
   8) Needs and expectations of key internal stakeholders
   9) Internal policies

C. Assess the processes related to the elements of the external environment in which organizations seek to manage risks and achieve objectives
   1) Key external factors (drivers and trends) that may impact the objectives of the organization
   2) Needs and expectations of key external stakeholders (e.g., involved, interested, influenced)

Source: The IIA International web site
Organizations and Organizational Culture

In order for organizations to establish a risk culture, it is first necessary to understand an organization as an entity. By simple definition, organizations are social entities that are goal-directed deliberately structured activities systems with permeable boundaries. More specifically, organizations as social entities are people or groups of people who function together to perform the tasks and functions of the organization so that the organization may reach its objectives.

Deliberately structured organizations objectives and goals are typically subdivided into subsets of activities. Hence, a different perspective of goals and objectives become apparent at the different levels within an organization. Although, with these different perspectives, these subdivided sets of activities should work toward the overall organization objectives and goals.

With this in mind, the deliberate structure of an organization should facilitate and coordinate the efforts of all of the subdivided sets and move uniformly toward one efficient and effective effort.

All organizations have permeable boundaries that at least should separate them from other organizations. This is called differentiation. This distinction defines individual organizations, functions, and purposes. In terms of competition, differentiation of purpose, product, or service will distinguish one organization from another. From the competitive perspective this differentiation is what will cause a customer or client to choose one company or organization over another. Some reasons for these customer/client differentiated choices could be price, location, customer service, quality, likeability of the company, and compatibility with customer needs and wants.

Organizations probably had more defined and distinctive boundaries in the past. However, in these more contemporary times the boundaries of organizations have become and must be more permeable or flexible. In order to survive it is now necessary that organizations share with each other information, cooperate, and collaborate. The sharing of technology, ideas, and components as well as international trade are just some examples of the necessity for more permeable boundaries of today’s organizations.

Further organizations can be subdivided into two distinct classes that directly relate to the organizations focus and ability to address their risk and hence their success. These classes of internal risk and external risk will be discussed later in detail. Internal risks include training; capabilities of staff and employees; the lack of physical controls such as locks, cameras; and passwords to name a few. Internal risks can be understood and fixed. Generally, there is or can be some control over internal risks.
External risks on the other hand are the elements that have an impact on the organization but that the organization has little or no control over. Consequently, the organization, although having little or no control over the advent of these external risks, must plan for and manage these external risks. External risks can include the environment, weather, interest rates, the economy, international relations, international suppliers, exchange rates, politics, and government rules and regulations.

The two subcategories of organizations that relate to both the internal and external risks are an open organization system and a closed organization system. A closed system does not depend on the environment in which it operates. The management of a closed system would be relatively simple to understand and manage; with no external influences to worry about, the closed organization system would most likely be stable and predictable. A closed organization would be totally autonomous, enclosed and sealed off from the outside world of external influences. Although possible, it is unlikely that a completely closed organization system by definition could exist in today’s business environment.

Answer the Following Question.

8. The Senior Vice President of Operations reports directly to the Chairman and President of Products Inc. This is a family-owned company which has grown substantially over the past few years. Now named Products International its growth can be attributed mostly to the purchase of three international companies. These newly-purchased companies provide similar products as the parent company and were also looking to expand to international markets. As all of these companies provide generally the same products which type of operating environment is Products International?

   a. product differentiation environment  
   b. open  
   c. conglomerate  
   d. closed

   See Application Questions, Answers & Explanations module for answer
Categories:

An open system must interact with the environment. This is a more likely situation in today’s environment. Open systems can be very complex and must require innovative and proactive management. Open systems have to find and obtain needed resources, interpret and act on environmental changes (external risks), dispose of outputs, control and coordinate internal and external activities, and manage environmental changes. Sometimes working closely with competitors and international markets their complexity increases. Remember as complexity increases so does risk.

Organizational structure definitions are fine to establish a framework for organizational culture but it is people, humans that make an organization function as it is intended. It is these people that establish the culture for such things as ethics, attitude, moral, risk management, and the establishment and implementation of adequate controls and move the organization toward its objectives most efficiently and effectively.

Connecting the tone:

Looking from the top-level of an organization downward, upper management is responsible for the entire organization. Upper management must establish objectives and goals, develop strategy, interpret the external environment, and adjust for the influences that the external environment imposes on the achievement of objectives. Further upper management must decided upon and influence the organization design and structure. In more detail, upper management must influence the entire organization toward compliance with laws and regulations, facilitate the accomplishment of goals and objectives, establish the reliability or information to internal and external stakeholders, manage the efficient and effective use of resources, and solidify the safeguarding of assets.

Probably most importantly is the tone that is established and emulated by top management. The words, speeches, posters, and newsletters are all fine but without a sincere tone of support and belief from top management, all of the words, speeches, posters, and newsletters are just that and will have little impact on the intended direction of the organization.

Next from the top down are middle managers. Middle managers are or should be concerned with the functioning of individual departments such as accounts payable, marketing, operations, and human resources to name a few. These middle managers must interrelate the functioning of their respective departments to the overall goals and objectives of the overall organization. These middle managers must design and implement effective interrelations of politics, technology, cooperation, along with risk and control management among interfacing departments.
Why the Concern with Third Party Relations?

Some Risks Associated with

Third-Party Relationships

Strategic risk. Strategic risk is the risk to earnings or capital arising from adverse business decisions or improper implementation of those decisions. Strategic risk can exist when there is an aggressive effort to remain competitive or boost earnings, and or use third-party relationships without fully performing due diligence reviews or implementing the appropriate risk management infrastructure to oversee the third party relationship. Strategic risk also arises if management does not possess adequate expertise and experience to properly oversee the activities of the third party.

Reputation risk. Reputation risk is the risk to earnings or capital arising from negative public opinion. Of all risks, this can probably be the most harmful both in the long and short terms. Third-party relationships that do not meet the expectations of customers or clients expose the company to reputation risk. Poor service, disruption of service, inappropriate sales recommendations, and violations of consumer law allowed by third party relationships can result in litigation, loss of business or both.

This is particularly true when the third party's employees interact directly with customers or clients and employ situations or actions are not consistent with the policies and standards of the parent company. In addition, publicity about adverse events surrounding the third parties may increase (reputational risk).

Compliance risk. Compliance risk is the risk to earnings or capital arising from violations of laws, rules, or regulations, or from nonconformance with internal policies and procedures or ethical standards. This risk exists when products, services, or systems associated with the third-party relationship are not properly reviewed for compliance, or when the third party’s operations are not consistent with law, ethical standards, and policies and procedures of the parent company.

Transaction risk. Transaction risk is the risk to earnings or capital arising from problems with service or product delivery. Transaction risk is evident in each product or service offered by the third party on behalf of the parent company. Transaction risk can increase when the products, services, delivery channels, and processes that are designed or offered by a third party do not fit with the parent companies, customer demands, or strategic objectives. A third party's inability to deliver, on behalf of the parent company, products and services, whether arising from fraud, error, inadequate capacity, or technology failure, exposes the parent company to transaction risk.
Summary:

Risk and control management and the achievement of overall objectives is the responsibility of everyone. However, in order for this to be successful upper management and the Board of Directors must recognize and manage the internal and external risk as well establish a risk appetite (the amount of risk that is willing to be accepted in order to achieve objectives). Further, it is the responsibility of the Board of Directors and management to effectively communicate and monitor this risk philosophy and culture to everyone.
### Organizational governance related to risk management

<table>
<thead>
<tr>
<th>1.3 when upper management is establishing a cultural philosophy they must understand and adjust for:</th>
<th>Answer 4 is the correct answer. The other answers are nice common words but do not apply to this question. The only answer that may even warrant some consideration would be answer 1. However, answer 1 is narrow only addressing the politics. Politics can be a risk but only one risk. Answer 4 implies multiple internal risks and external risks. It is much better to understand the implications of as many internal and external risks as possible when developing cultural philosophy.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. internal and external politics</td>
<td></td>
</tr>
<tr>
<td>2. internal controls</td>
<td></td>
</tr>
<tr>
<td>3. feedback</td>
<td></td>
</tr>
<tr>
<td>4. internal and external risk</td>
<td></td>
</tr>
</tbody>
</table>
DOMAIN II:
PRINCIPLES OF RISK MANAGEMENT PROCESSES
EXTRACT
Domain II: Principles of risk management processes

The objective of this module is to better prepare the participant to pass the Certification in Risk Management Assurance Exam by discussing and analyzing the technical dimensions of this domain while discussing techniques to best manage multiple-choice questions.

Included are discussions of the skill requirements of a CRMA to:

A. Benchmark risk management processes using authoritative guidance

B. Evaluate risk management processes related to:

1. Setting objectives at all levels to achieve strategic initiatives
2. Identifying risks
3. Risk analysis and evaluation including correlation, inter-dependencies, and prioritization
4. Risk response (e.g., avoid, transfer, mitigate, accept), including cost/benefit analysis
5. Developing and implementing risk mitigation plans
6. Monitoring risk mitigation plans and emerging risks
7. Reporting risk management processes and risks, including risk mitigation plans and emerging risks
8. Periodic review of risk management processes to aid in continuous improvement

Source: The IIA International web site
Principles of Risk Management Processes

Managers put assets at risk to achieve objectives.

Establishing Objectives

Establishing objectives should be the first step in any business process. Establishing objectives has to be the first step whenever performing a review of business risks or a risk or control analysis. If the objectives are overlooked, the efforts will be wasted.

Back to basics: These are the three basic elements of business objectives, risks, and controls which should be addressed in that order. The very first element and the foundation necessary to be able to address the implementation and adequacy of risk management is an objective. Any process, physical task, or human effort must have an objective, a clear focus of what is trying to be accomplished.

Some of the general terms associated with the establishment of objectives, in order of decreasing detail are the mission statement, the objectives, and goals.

Generally, the amount of detail to accomplish the objectives increases with the definition of goals. However, no matter if the mission, objectives, or goals are being discussed it is necessary that a clear focus of what it trying to be accomplished be kept in mind.

Objectives Must Be Specified First, if objectives are not specified first

- risk will become overwhelming
- risk may not be controllable
- efforts and resources will be wasted
Below are the criteria, most often associated with the definition of goals. However, they can be utilized for establishing adequate objectives as well:

**Specific:** means that a definitive outline of what is to be accomplished be identified. The more specifics that are identified the more likely the objectives will be accomplished effectively and efficiently. Conversely, the less specifics that are identified the less likely the objectives will be accomplished as intended. With fewer specifics, humans will interpret a direction, which may not be in concert with the overall objectives. Hence, inefficiencies will prevail.

**Measurable:** the action to accomplish objectives is subject to technological and human intervention. Therefore, it is important that a measurable mechanism be put in place to monitor these actions to insure that the intended objectives are being accomplished. As with any monitoring control the monitoring control should not only include a physical monitoring mechanism but as well an action to adjust deviations beyond accepted limits. For extensive objectives, (those which may take an extensive time to complete) benchmark / status measurements are appropriate. This means that periodic measurements at predetermined times be established. These benchmarks / status measurements will help to guide minor adjustments as they are recognized as opposed to waiting until major adjustments are required.

Additional comments about benchmarking: **benchmarking is the measuring or comparing of an entity, process, or objective against another real or perceived entity, process, or objective.** Benchmarking measures progress among or between these relationships. Benchmarking can help establish priorities, targets, and the need for adjustments in the process.

**Some uses of benchmarking:**

- develop performance measures
- develop comparisons of performance relative to goods and services
- access ideas from proven practices
- develop best practices
- maintain a competitive advantage
RISK ASSESSMENT APPROACH

WORK UNIT OBJECTIVES

ORGANIZATION'S OBJECTIVES

2-way link

WORK UNIT OBJECTIVES

ORGANIZATION MISSION/PURPOSE

ENVIRONMENTS
- Political
- Customer/Constituent
- Suppliers
- Technology
- Government Regulations
- Competition
- Economic/Financial
- Physical

KEY PROCESSES
- Transforming
- Safeguarding
- Measuring
- Communicating

MANAGEMENT PROCESS AND CONTROL

WORK UNIT ASSETS

ASSET TYPE
- Physical
- Financial
- Human
- Information/Intangible

SIZE/VALUE LOCATION PORTABILITY

Source: David McNamara, "Risk Management and Risk Assessment"
Risk Terms

Risk is a concept. It is a measure of uncertainty (probabilities). In business processes the uncertainty involves the achievement or the barriers to achieve organizational objectives. Risk may have positive or negative consequences. Generally, positive consequences are known as opportunities and negative consequences are called threats or risks.

Consequences are tangible outcomes of risk on the decisions, events, or processes. Although it can be difficult to identify and measure the intangible risk, (sometimes called soft issues, like lack of moral, bad work ethics, in adequate management style and others) we can and should anticipate the implications of these soft issues. Risk is neither good nor bad, it just "is."

Consequences can vary in severity depending on a number of factors, some of these factors are:

- the assets at risk
- the type of threat
- the duration of the consequence
- the effectiveness of controls in place

Exposure is the susceptibility to loss or a perception of a threat to an asset or asset-producing process. Generally, the more valuable the asset is to achieving the organization's established objectives, the more important that exposure becomes. Exposure is controlled or diminished by adequate and effective risk management techniques, including designing and maintaining effective controls.

Threat is a combination of the risk, the consequence of that risk, and the likelihood that the negative event will take place. The type of threat is actually an expression of the type of consequence such as fire, flood, error, omission, delay, fraud, breakdown, and obsolescence. Threats come from the operation of risk in the environment, regardless of the controls or control environment. Threats are always present; controls keep them in check (as long as the controls are effective).

The duration of the consequence affects its severity. This can be well described with an example of a computer center. Most computer center managers will tell you, if the computer is down for an hour, that's one consequence. However, if the computer is down for a day that's another, and if it is down for a week that is another and much more severe!
The Concept of A Control Cannot Exist Without A Clear Focus on The End Achievement

Integrated Control Frameworks

Integrated control frameworks can help identify, measure, and prioritize risk in multiple and related dimensions of a process. Consequently, they help identify needed controls in these dimensions of the process.

Control Frameworks and Rules and Regulations an Overview

As a reactionary control, because of multiple control breakdowns, in business and government integrated control frameworks began to evolve. One of the first to emerge was produced by The Committee of Sponsoring Organizations (COSO) of the Treadway Commission headed by James Treadway. This integrated control framework became know as COSO.

The COSO independent commission summoned input from various business and government professionals. Their purpose was to develop a standardized risk and control framework which could be applied to any business or process.

In addition to providing a standard for risk and control management, which had been inconsistent to this point among businesses and government entities, this framework would introduce a new concept in risk and control management. Incorporated in the framework was integration. This meant that risk and controls would now be evaluated across and vertically in multiple entities of an organization.

With COSO risk and controls would now be evaluated in a holistic view of an entire organization including how various entities synergized or did not synergize for a common objective.

It was realized that the root cause for inadequacies in the hard controls actually resided in the adequacy or inadequacy of the soft controls. A new component of risk and control management was also introduced with the advent of COSO. COSO encourages a sincere evaluation of the soft controls and issues.

Traditionally risk and control professionals evaluated the more tangible controls (the hard controls). The evaluation of these soft controls generally was a new concept to traditional risk and control and business professionals. Assessment of these soft controls now would require professionals to evaluate such things as morale, ethical values, attitude, management philosophy, and employee competency.
2.4 Which of the following best describes the three basic parts of a business process?

1. in order to achieve anticipated objectives, controls must be managed appropriately
2. objectives must always be considered independently
3. the management of risk will help achieve objectives
4. appropriate and timely management of risk, combined with the appropriate management of controls and common sense works best

Answer 4 is the correct answer. Answers 1 & 3 could be considered correct but using the words “appropriately” and “timely,” answer 4 has a broader scope. The right amount of controls and when they are applied is important in an adequate control process. Answer 2 is incorrect because controls should not be considered independently - they are part of a process.
DOMAIN III:
ASSURANCE ROLE OF THE INTERNAL AUDITOR (IA)
EXTRACT
Domain III: Assurance role of the Internal Auditor (IA)

The objective of this module is to better prepare the participant to pass the Certification in Risk Management Assurance Exam by discussing and analyzing the technical dimensions of this domain while discussing techniques to best manage multiple-choice questions.

Included are discussions of the skill requirements of a CRMA to:

A. Review the management of key risks
B. Evaluate the reporting of key risks
C. Provide assurance that risks are adequately evaluated
D. Provide assurance on risk management processes
Assurance role of the Internal Auditor (IA)

The 1999 IIA Standards states that each internal audit organization should define both assurance and consulting services in terms of what is appropriate for their own organization, and those definitions should be formal and published in the internal audit charter.

The IIA Standards clearly identify the opportunity for internal audit to increase its contribution to the success of an organization by using assurance to add value and improve an organization’s operation in a consulting

“Internal auditing is a …assurance activity designed to add value and improve an organization's operations. …”

Source: 1999 IIA Standards from www.theiia.org

Internal audit helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

Assurance:

The role of assurance is a natural extension of what internal auditors already accomplish. They must offer professional services to survive in an extremely competitive business environment. Both have “some independence” but are dependent of payment for services. Both operate on project basis with a start and completion date (an audit is an example).

The review, evaluation, and management effort of key risks in a process is easier said than done. To be effective this effort requires collaboration between and among process owners and risk and control specialist (internal auditors) at all levels. This means that there must be an understanding and acceptance by process owners of how to identify, measure, and prioritize key risks and then act on them accordingly. In addition, this effort requires an empathetic approach by the risk and control specialist to help the process owners gain an understanding of risk and control management. It is not only the risk and control specialist that are or should be identifying, measuring, and prioritizing key risks.
Continuous Monitoring

One of the roles that internal auditor plays in the area of risk management is to help process owners continually improve their processes. Internal audit can meet process owners’ expectations by expanding use of operational auditing and traditional auditing skill to apply internal audit knowledge about controls.

Process owners with an ever-increasing list of required tasks will welcome helpful suggestions as to how to improve their processes.

Operational Auditing

The Terminology Jungle

The expansion in the scope of internal auditing though took place in a very short span of time, yet it manifested itself in a spurt of terms and expressions. People started talking of operational auditing in different words. Some of the more common expressions were:

- operational auditing
- comprehensive auditing
- value-for-money auditing
- management auditing
- operations auditing
- efficiency auditing
- effectiveness auditing
- preventive auditing
- system-oriented effectiveness auditing
- operational evaluation
- project auditing
- program auditing
- program evaluation
There is a need for internal audit to monitor both business risks and IT risk. This eliminates the audit risk of “over auditing” and “under auditing” the same business process, redundant recommended control techniques, unreported risks in those areas where neither the IT auditor nor the auditor thought were their responsibility, and a significant waste of resources. The goal of Integrated Audit has been around since the 1970s. They are internal auditors who understand both business and IT risk. These understanding can be accomplished by a team of internal auditors.

The key question is “Who Does What?” Computer-based auditing will significantly improve internal audit’s abilities to provide continuous monitoring (auditing).

If it is a computer-based process then internal audit needs to use computer-based auditing

Source: John Tongren, “Exceeding Expectations for Internal Auditors”
3.3 CSA is a process that will ensure:

1. that business objectives are met
2. that risk is addressed
3. that appropriate controls will be put in place
4. none of the above

Answer 4 is the correct answer. The word “ensure” is the giveaway in this question. CSA is a control tool that addresses risks and the achievement of objectives. However, it is virtually impossible to protect against all risks all of the time. Therefore, answer 4 is the best answer.
DOMAIN IV: CONSULTING ROLE OF THE INTERNAL AUDITOR (IA) EXTRACT
Domain IV: Consulting role of the Internal Auditor (IA)

The objective of this module is to better prepare the participant to pass the Certification in Risk Management Assurance Exam by discussing and analyzing the technical dimensions of this domain while discussing techniques to best manage multiple-choice questions.

Included are discussions of the skill requirements of a CRMA to:

A. Facilitate identification and evaluation of risks
B. Coach management in responding to risks
C. Coordinate risk management activities
D. Consolidate reporting on risks
E. Maintain and develop the risk management framework
F. Advocate for the establishment of risk management
G. Develop risk management strategy for board approval
CONSULTING ROLE OF THE INTERNAL AUDITOR (IA)

The 1999 IIA Standards states that each internal audit organization should define both assurance and consulting services in terms of what is appropriate for their own organization, and those definitions should be formal and published in the internal audit charter.

The IIA Standards clearly identify the opportunity for internal audit to increase its contribution to the success of an organization by using consulting to add value and improve an organization’s operation in a consulting role.

“Internal auditing is a …consulting activity designed to add value and improve an organization's operations. ...”

Source: 1999 IIA Standards from www.theiia.org

Consultant:

The auditor as a consultant has long been debated. The question is, should internal auditors act as consultants or not? In practice, some audit departments say “no” and some say “yes”. In addition to further complicate this debate the need or opportunity for internal auditors to act as consultants changes with the needs of the business. Therefore, at any one point in time, an audit department that says “yes” may at another time say “no”. An audit department that at one point in time that says “no” may at another time say “yes”. This change in opinion is most often a result of business needs and leadership.

Therefore, with all this confusion, it is probably best to understand what internal auditors actually do, what consultants do, and how the professional practices from the Institute of Internal Auditors provide guidance.
This definition is sometimes difficult because each person seems to have a definition of consultant based on that person’s business and personal experience. This definition is also difficult because of the many types of consultants including those making a small hourly wage, those making 100s of dollar an hour, those working for major firms, those working for small organization, self-employed individuals, and a seemingly endless number of variations of these.

To discuss the consulting role of the internal auditor related to risk management it is important to define what a consultant is and what a consultant does. Then a comparison can be made between an auditor and a consultant. Taking an increased involvement in risk management does not imply that the internal auditor abandons auditing but that they increase their opportunities and the benefits to the clients by increasing their use of consulting skills. One approach to define a consultant is to use a dictionary that contains the following definition.

**Dictionary definition of consultant**

“… one who offers professional advice or professional products …”

Using this definition it is clear that internal auditors are already acting as consultants as the only purpose of internal audit is to provide professional advice and products (like audits and other services) to the organization. Providing advice related to risk management is to continue to provide that advice and those services or to expand the internal audit role further.
Summary:

Internal audit’s in-depth knowledge of internal controls has created excellent opportunities for internal audit to provide education or training to all levels of an organization from the board of director to direct supervisor about many of the features of risk management including services that internal audit can provide. These services are available because the fact that internal audits are performed throughout an organization providing unique views of risk gained from a history of audits in all of the many areas of an organization.
Consulting Role of the Internal Auditor (IA)

<table>
<thead>
<tr>
<th>4.2 The risk formula to determine the probability of a control failure is:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. modified annual loss expectancy</td>
</tr>
<tr>
<td>2. annual loss expectancy</td>
</tr>
<tr>
<td>3. direct probably estimate</td>
</tr>
<tr>
<td>4. modified risk versus control failure probability</td>
</tr>
</tbody>
</table>

Answer 1 is the correct answer. First, answer 4 can be eliminated. Although it may sound relative to risk assessment and this question it is just a set of random words. Of the three remaining answers answer 1 the modified annual loss expectancy is the correct answer and the formula that will help determine the probability of a control failure.
Suggested Additional References

Review courses by themselves including the McKeever CRMA Study System are generally not sufficient to ensure exam success. This study system will certainly provide you with an approach to significantly improve your chances of passing.

Several references to additional material appear within the McKeever CRMA Study System.

The IIA web site lists a variety of study material to use to help you pass both the CRMA Exam and Part 1 of the CIA Exam.

Following is a listing from The IIA website www.theiia.org of 19 references that you might also consider as additional study material for passing the CRMA Exam.
Appendices Extract

Note:

This module is designed to provide subject supplemental study material in the areas:

1) Some Probing Questions to Help Understand Client’s Problems
2) Diagnostic Questions to Help Understand Client’s Problems
3) Some Comments about Sampling Useful in Risk Management
4) Financial Ratios Useful in Risk Management
5) Financial Institution Regulations Related to Risk Management
Note:

This module is designed to work with the Application Questions, Answers & Explanations module.

Read and consider each question in any sequence.

Answer that question the best that you can.

Then check your answer and read the explanation for that question in the Application Questions, Answers & Explanations module.

This process both reinforces your understanding of the material and improves your test-taking technique.
6. During a recent risk assessment exercise, utilizing a team of process owners, a discussion of how to address the interrelationship risk among the processes began to escalate. It seems that the process owners could not agree on the risks that should be addressed. What was most likely a reason for this lack of focus?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>the process owners do not understand the consequences of risk</td>
</tr>
<tr>
<td>b.</td>
<td>the process owners do not understand the overall objectives of the processes</td>
</tr>
<tr>
<td>c.</td>
<td>the process owners should identify, measure, and prioritize the risks</td>
</tr>
<tr>
<td>d.</td>
<td>the process owners should work in smaller teams to discuss risks in the individual processes then work as a group</td>
</tr>
</tbody>
</table>

See Application Questions Answers & Explanations module for answer
Application Questions, Answers & Explanations

Note:
This module is designed to work with both the Application Questions module and Domain modules and.

Review each question you see in either module.

Answer that question the best that you can.

Then check your answer and read the explanation for that question in this module.

This process both reinforces your understanding of the material and improves your test-taking technique.
6. During a recent risk assessment exercise, utilizing a team of process owners, a discussion of how to address the interrelationship risk among the processes began to escalate. It seems that the process owners could not agree on the risks that should be addressed. What was most likely a reason for this lack of focus?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>a.</strong></td>
<td>the process owners do not understand the consequences of risk</td>
</tr>
<tr>
<td><strong>b.</strong></td>
<td>the process owners do not understand the overall objectives of the processes</td>
</tr>
<tr>
<td><strong>c.</strong></td>
<td>the process owners should identify, measure, and prioritize the risks</td>
</tr>
<tr>
<td><strong>d.</strong></td>
<td>the process owners should work in smaller teams to discuss risks in the individual processes then work as a group</td>
</tr>
</tbody>
</table>

Answer **b.** is the correct answer. Answers **c.** & **d.** are not relevant to this question. Answer **a.** would seem like a reasonable choice especially since the word risk is included in the answer statement. However, the question implies that an interrelationship of risk among processes is being discussed and not agreed upon. This would mean that there was a lack of understanding of the overall objectives. Now answer **a.** is very specific. However, it only implies that the team does not understand the consequences of risk. It does not indicate that this is the risk relative to the interrelationship among processes. Watch the wording and think about the answers before making a quick choice.