RIMS-CRMP

RIMS-Certified Risk Management Professional

RIMS-CRMP Study Guide

Certification Programs

228 Park Ave S PMB 23312, New York, NY 10003-1502

(212) 286-9292 | RIMS-CRMP@RIMS.org

www.RIMS.org

ANAB

ANSI National Accreditation Board

ACCREDITED

ISO/IEC 17024

PERSONNEL CERTIFICATION BODY

RIMS

the risk management society

Table of Contents

Tables and Figures

Introduction

Thank you for your interest in the RIMS Certified Risk Management Professional (RIMS-CRMP) examination administered by RIMS, *the* risk management society®.

In order to qualify for the RIMS-CRMP examination, you must meet the eligibility requirements detailed in the Candidate Handbook, and listed on the RIMS-CRMP website. The Candidate Handbook provides detail on eligibility requirements, examination logistics, recertification requirements, the Code of Ethics and additional policies. The Candidate Handbook is available on the RIMS website at:

www.RIMS.org/links/candidatehandbook

The purpose of this document is to serve as a study guide for anyone who is taking the RIMS-CRMP certification examination. It is not intended to replace any textbook or other resources you need to prepare for the examination, and using this guide does not guarantee that you will pass the examination. The study guide is divided into two sections. The first section deals with the background of the RIMS-CRMP certification and provides guidance on the process of studying, taking the examination, and what to expect at the testing centers.

The second section summarizes five core competencies of a risk professional:

1. Analyzing the Organizational Model
2. Designing Organizational Risk Strategies
3. Implementing Risk Process
4. Developing Organizational Risk Competency, and
5. Supporting Decision Making.

It then reviews each of the core competencies based on five review components:

1. Learning objectives
2. Examples
3. Recommended reading
4. Self-assessment of content areas, and
5. Sample exam questions

The study guide concludes with a glossary of terms and bibliography.

Section 1 – Background and Process

About the RIMS-CRMP Certification

RIMS, the risk management society®, is a global not-for-profit committed to advancing the practice of risk management throughout the world. RIMS brings networking, professional development, certification, and education opportunities to its membership of 10,000 risk management professionals in over 60 countries. Founded in 1950, the Society represents more than 3,500 industrial, service, nonprofit, charitable, and government entities throughout the world.

The RIMS-CRMP certification distinguishes the achievement of validated risk management competencies of an effective risk management professional. The RIMS-CRMP is based on a job task analysis completed by dozens of experienced risk management experts. It has been statistically and psychometrically validated by a global representation of RIMS members. Achieving the RIMS-CRMP credential represents a unique combination of experience, demonstrated knowledge and competency in risk management, and dedication to upholding high standards of ethical and professional conduct. Individuals who earn and retain the RIMS-CRMP certification are required to: attest to the certification requirements through an application, provide supporting documentation, pass a rigorous exam, uphold an established Code of Ethics and meet continuing education requirements in order to maintain the certification. Typically RIMS-CRMPs have expertise in a specific field of risk management and want to differentiate themselves as an acknowledged professional by earning the RIMS-CRMP certification.

RIMS-CRMPs may use the credential to establish credibility within their organizations, among other professionals and with the public. Adding the RIMS-CRMP certification to your professional profile demonstrates that you have achieved a high level of competency through validated expertise, education and experience to successfully manage risk and create value for your organization. Let's get started!

Study Strategies

People review and process information in different ways. Some individuals find memorization easy, while others sort facts into a contextual framework. The RIMS-CRMP examination requires that you know factual data and use the information in decision-making and in problem-solving situations.

Learning styles differ. Some individuals prefer to study alone, while others prefer a study partner or study group. Discussing information with a partner or in a group can help clarify, process and integrate information. Some individuals learn better by hearing information, while others learn better by reading or writing information.

Research methods vary. How do you tackle unfamiliar topics? If you hear about something exciting and want to learn more, how do you go about finding information? Do you read about it, take a class, call an expert and ask for a demonstration, or purchase equipment and teach yourself? Some prefer one method over another. For example, if you chose to ask an expert, then you may prefer a hands-on approach where you can safely experiment (trial and error) and get input and feedback from someone knowledgeable in that area. Others choose a combination of methods. For example, you can attend courses, view webinars that can be repeated, highlight texts or write flash cards that can be reviewed.

Study groups can drive accountability. Whoever leads the group may utilize this study guide and/or additional resources. A group of people can talk through ideas, provide examples and support each other in their learning endeavors.

Formulate a study strategy and schedule sufficient time to prepare. You are the best judge of your study preferences, so use what works best for you.

Approaches to Memory and Retention

This section outlines some tips for memorization and retention. While the RIMS-CRMP examination is not based on "rote-learning" and memorization, using these types of techniques can prove effective to remember and recall pertinent concepts and facts. These techniques may help in preparing for this exam, as well as help you for other learning purposes.

Memorization and recall is a key component of studying. While you may already possess the practical knowledge, recalling it during a time of stress may prove challenging.

One key strategy to recalling information is to self-test. As you compile and address content areas from the exam, a theory called "the testing effect" shows that learning is enhanced by the act of recalling information after exposure[1]. This simply means that by reading information, recalling and reviewing as much as possible (self-test) and then re-reading the information, retention was found to be greater than just reading and taking notes.

Other techniques associated with recalling information are:

1. **Get organized.** Organize notes according to domain and content area. Find a quiet, uncluttered space in which to study. If you are studying in a group, make sure the group space is free from distractions from outside noise, chatter and clutter.

2. **Make it meaningful.** Create mnemonic devices to help recall formal names of concepts. Various types of devices include rhyming (I before E except after C...), names (ROY G BIV = colors of the rainbow), or notecards. It's also best, when possible, to relate a concept to a personal experience. If personal experience is attached, the concept holds more meaning therefore it may be recalled more readily.

3. **Don't cram.** Spread studying out over several days or weeks. Study in chunks of time. Do not spend three, four, or five consecutive hours studying. Take frequent breaks (every 20-25 minutes) to refresh and recuperate.

4. **Take notes and create flashcards.** While most people have a laptop at their disposal, research shows that taking notes by hand is better than taking notes on a laptop for remembering conceptual information over the long term[2]. The old-fashioned method of taking notes by hand forces you to synthesize information in ways that typing doesn't.

5. **Get enough sleep.** The right amount of sleep aids in better performance, mental agility and wards off stress. The brain converts facts from short-term memory into long-term memory while sleeping.

Strategies for Analysis of an Exam Question

All questions on the RIMS-CRMP examination are in the four-choice multiple-choice item type format. This item format consists of a stem, which is in the form of a question or incomplete statement, and four response options. Only one of the response options correctly answers the stem (the key); the other three options are incorrect (the distractors). When responding to the questions on the RIMS-CRMP examination; you select ONLY one of the response options.

The questions on the RIMS-CRMP examination may vary in complexity. Some questions ask you to recall information (such as, "What is X?") and some questions require you to apply knowledge in order to select the most appropriate response or action given the situation in the stem. When responding to each question, you should always select the BEST option. You should also pay close attention to the words in the stem, to determine what the question is truly asking, as the question may be asking what MUST be done or what is MOST commonly done vs. what CAN be done.

[1] Dobson, John L., and Tracy Linderholm. "Self-testing Promotes Superior Retention of Anatomy and Physiology Information." Advances in Health Sciences Education 20.1 (2014): 149-61.

[2] Mueller, P. A., and D. M. Oppenheimer. "The Pen Is Mightier Than the Keyboard: Advantages of Longhand Over Laptop Note Taking." Psychological Science 25.6 (2014): 1159-168.

Each question on the exam is written so that all four answers are plausible. If this was not the case, and the incorrect answers were implausible, then your knowledge would not be effectively measured. The exam does not use "trick" questions. Instead you must either know the data or be able to effectively apply the data in a decision-making process to choose the BEST answer.

All questions and answers are referenced to a recognized and accepted textbook or resource. Each question has been reviewed by a number of experienced professionals in the field who agree on the correct answer. In addition, a substantial amount of empirical data has been collected on each question to assure that it performs appropriately and effectively. The four answers presented may not agree with your individual interpretation of the material. Regardless, it will be necessary to choose one of the four answers provided as the best answer.

Being familiar with how test items are constructed may help when analyzing a question or choosing a correct answer if stuck. More information about how multiple choice items are developed can be found here:

https://cft.vanderbilt.edu/guides-sub-pages/writing-good-multiple-choice-test-questions/

General Strategies for Taking the Exam

Prior to the exam:

Prepare for the multiple-choice exam by employing a variety of test-taking strategies. These strategies do not guarantee passing the exam, but they will give insight as to how you can interpret questions and evaluate information:

Test strategies:

- Read the directions carefully.
- Know how much time is allowed. Time limits govern strategy.
- If time allows, review both questions and answers. It is possible to misread questions the first time.

Answering options:

Improve your odds by thinking critically. Cover the options, read the stem, formulate an answer, and select the option that most closely matches your answer. Strategies for answering difficult questions include:

1. Eliminate options you know to be least incorrect.
2. Give each option of a question the "true-false test." This may reduce your selection to the best answer.
3. "Eliminate look alike options." Choose the best answer but disregard choices that mean basically the same thing, and thus cancel each other out.
4. Compare alternatives for differences. If two alternatives seem correct, compare them for differences, then refer to the stem to find your BEST answer.

Remember that you are looking for the best answer not only a correct one, and not one that must be true all of the time, in all cases, and without exception.

Test Preparation Strategies

References provided throughout the review section do not constitute a required reading list. The important topics that you should study to successfully prepare for the examination are listed in the examination blueprint of core competencies found elsewhere in this guide. You are strongly encouraged to carefully review the examination blueprint to identify topic areas that may require extra review and study.

Moreover, learning objectives and examples provided in this guide have been developed independently of the examination questions. Rather than representing an exhaustive list of learning objectives or examples, their use is meant to create a starting point for you to think about the concepts in a way that not only helps you retain information to take a test but also to understand the competency areas you want to focus on.

As you prepare for the RIMS-CRMP certification examination, use the examination blueprint to build your study plan. The blueprint contains the major competency areas on the exam, and the percentage of the exam each competency area represents. You can decide what you want to read and study based on your current experience and knowledge about risk management to determine how much preparation is required for each topic area of the examination.

Ask yourself these questions:

- Which competency areas represent the greatest number of test questions? The greater the number of possible questions on the exam, the more focus you may need on these topics to prepare.
- How much time do I need to focus on these areas to prepare for the exam versus other areas? For example, if there is only one question on a specific item, it would not make sense to spend 50% of study time on that topic.
- How do my current knowledge and skills compare to the competency areas of the exam? Am I strong in some, but weak on others? Making this assessment will help budget study time.
- How much training or work have I done in the areas on the exam? Extensive training and/or experience in a specific area will lower the priority of studying them further.

Analysis of the examination blueprint and your answers to the questions above will help determine where you need to spend study time. When your preparation is complete, and after receiving confirmation that your application for the RIMS-CRMP was approved, you should schedule an appointment at an approved testing center to take the examination.

What to Expect on Exam Day

Preparing for the day of the in-person exam:

- Find the test location before test day. Allow for extra time for unforeseen events such as traffic.
- If you have considerable distance to travel, consider arriving the day before.
- Get a good night's rest.
- Eat a well-balanced meal prior to reporting to the exam site. Avoid excessive stimulants such as caffeine.
- Plan to arrive at the exam site at least 30 minutes prior to your appointment to allow plenty of time for registration and processing.

Preparing for the day of the OnVUE online proctored exam:

- Get a good night's rest.
- Eat a well-balanced meal and avoid excessive stimulants such as caffeine.
- Check in 30 minutes in advance.
- Conduct a systems check to make sure your computer is ready.
- Clear your work area of notes and study materials.

What you will need to bring:

Authorized candidates who are taking the RIMS-CRMP examination at a Pearson VUE testing center or via OnVUE online proctoring will be required to provide one form of valid identification (ID). ID must contain a photo and signature. The first and last name used to register must match exactly the first and last name on the ID that is presented on test day.

Acceptable Forms of ID
• International Travel Passport
• Driver's license
• Military ID (including spouse & dependents)
• Identification card (national/state/province identity card)
• Alien registration card (green card, permanent resident, visa)
• Local language ID (not in Roman characters) – accepted only if issued from the country the candidate is testing in

* The ID must contain a photo and signature unless the signature is embedded in the identification. When this occurs, the candidate must present another form of signature identification from the list, e.g., a passport AND a government-issued driver's license OR state/national identification card with photo and valid signature AND signed credit card.

Please check the Pearson VUE website when scheduling an appointment to determine if there are additional instructions regarding identification requirements at the chosen test center. If you have any questions about the ID you are required to bring with you to the testing center for admittance for your exam, please contact Pearson VUE customer service at ***www.pearsonvue.com/contact****.*

During the exam:

The Test Administrator or online proctor will keep the official time and ensure everyone is given the allotted time of two hours for the examination. If anyone leaves the room, for example, to take a restroom break, the examination time will not stop. Restroom breaks are not permitted for online proctored exams. Proctors will monitor the exam.

- Read and follow the instructions carefully. Ask the proctor for clarification if you are not sure about the instructions. Remember, the proctors cannot and will not answer questions related to exam content.
- Periodically check your progress. This will allow time for you to make adjustments.
- You may go back to review any items, so mark questions you wish to review if time permits.
- Pay attention to reminders of the time you have left to finish the exam.

If you have questions or concerns about a test item during the examination, you may leave a comment by clicking the "comment" button on the computer screen or by chat for online proctored exams.

Rules at the test center and online proctored exams:

No one is permitted to leave the examination area to go to a car, to speak to anyone, or to make personal calls. The Test Administrator may dismiss an individual from the examination for any of the following reasons:

- If admission to the examination is unauthorized.
- If the individual creates a disturbance or gives or receives help.
- If the individual attempts to remove examination materials or notes from the testing room.
- If the individual attempts to take the examination for someone else.
- If the individual has in his or her possession any prohibited item.
- If the individual exhibits behavior consistent with memorization or copying of examination items.

Additional rules for online proctored exams:

- The testing area should be in a walled room with a closed door.
- Individuals other than the candidate may not see the computer screen that presents the examination questions.
- If another person enters the room during testing, the exam will be terminated.
- Candidates are not permitted to leave the room during testing. Breaks are not allowed during testing for any reason. If the candidate leaves the room, the proctor will end the session and the candidate will be unable to continue testing.
- Water in a clear glass is allowed during testing; however, eating, smoking, and chewing gum are prohibited.

All examination questions are copyrighted property of RIMS. It is forbidden under applicable copyright laws to copy, reproduce, record, distribute, display or share these examination questions by any means, in whole or in part. Doing so may subject you to severe civil and criminal penalties and actions by the RIMS organization.

If the exam is computer-based, results (pass/fail by domain) may be provided to you before you leave the test center. Otherwise, you will be notified post-exam. Timing of notifications may vary.

To view a short video of test-taker tips and what to expect for both the test center experience and OnVUE online proctoring, please visit: **https://www.pearsonvue.com/us/en/test-takers/resources.html**

Section 2 – Examination Blueprint and Review Components

Summary of Examination Blueprint

Table 1 depicts the five domains — also referred to as core competency areas — and some of the key duties and tasks associated with each domain. The columns on the right side of the table show the percentage weight each domain has within the overall exam, and each task within each domain have based on the number of potential exam questions. The weighting will help you prioritize study time and identify opportunities for personal improvement. For example, the domain of "implementing risk process" represents slightly over a third of the exam, and its six duties and tasks are almost equally weighted. On the other hand, the domain of "analyzing the business model" represents 15% of potential exam questions, and of its seven duties and tasks, three are more heavily weighted: obtaining internal organizational information, analyzing operations, and understanding value chain.

Table 1 Domains and Key Duties

Duties and Tasks	Final
A. Analyzing the Organizational Model	**16%**
A.1 Obtain internal organization information	
A.2 Obtain external information about organization	
A.3 Conduct internal analyses on the organization	
A.4 Assess organizational resilience	
B. Designing Organizational Risk Strategies	**26%**
B.1 Determine risk appetite and tolerance	
B.2 Develop risk strategy approach	
B.3 Define organizational risk competency and capabilities	
B.4 Design risk management framework	
B.5 Obtain organizational support for risk strategy	
B.6 Design implementation plan	
B.7 Develop risk communication plan	
C. Implementing Risk Process	**32%**
C.1 Identify scope, context, and criteria	
C.2 Identify risks and opportunities	
C.3 Analyze identified risk	
C.4 Evaluate risk	
C.5 Collaborate with stakeholders to identify risk solution options	
C.6 Monitor organizational risk	
D. Developing Organizational Risk Competency	**16%**
D.1 Engage organization's risk network	
D.2 Deliver risk training	
D.3 Coach organization on the risk process and techniques	
D.4 Continuously improve risk management process	
D.5 Integrate risk management into day-to-day operations	
E. Supporting Decision Making	**10%**
E.1 Influence risk-based decision making	
E.2 Advise on risk and resilience decisions	
Total	**100%**

For review purposes, the domains may be viewed as sequential where competencies in one domain are needed to demonstrate competencies in the next domain. For example, you could say that you

"Analyze the business model" so that you can

"Design organizational risk strategies" so that you can

"Implement risk process" so that you can

"Develop organizational risk competency" so that you can also

"Support decision making" throughout the organization.

In reality, competencies in one domain reinforce competencies in each of the other domains. For example, the competencies within the decision-making domain strengthen the first domain of competencies regarding (on-going) analysis of the business model. In fact, in a dynamic business context, changes in the decision making domain could result in competency refinements within any or all of the other domains.

Figure 2 is a graphical representation of domains within the RIMS-CRMP competencies reinforcement loop. Keep in mind that the domains do not represent a standard, nor do they represent a risk management framework, per se. Their primary purpose is to communicate the core competencies associated with effective risk management as psychometrically validated through the RIMS-CRMP development process.

Graphical Representation of Core Competencies of the RIMS-CRMP Certification

Figure 2

Review Components

Detail on each domain is broken down into five areas in order to aid the studying process.

1. Learning objectives provide more detail around the tasks identified in the exam blueprint.
2. The examples section provides more detail in the form of definitions and examples.
3. The recommended reading section provides useful recommendations on books, articles, white papers, and other material that will help you learn concepts more thoroughly and find more examples.
4. The self-assessment offers you an important opportunity to self-rate your competency in each domain area generally and each competency more specifically. Appendix A contains a sample that can be used to track your progress over time, as well as a self-assessment worksheet.
5. The sample exam questions are actual questions from the test bank utilized for certification and give a real-life look at how questions are worded and show the source that supports the answer to the question.

Section 3 – Review

Domain 1: Analyzing the Organizational Model

The first domain in the RIMS-CRMP core competency model addresses analysis of the organizational model. The analysis identifies the value proposition of the organization and the reasons customers buy a product or a service, and in the case of non-profits why donors give money, time, and ideas. Investigating the purpose of an organization answers important questions about the products or services the organization will deliver; its customers, target markets, and anticipated expenses and risks to delivering products and services. The first domain provides a solid foundation for the remaining domains because scrutinizing expenses and risk is not just about ensuring the organization will be a going concern but identifies how the organization should be resilient and focus on long-term stability in pursuit of its objectives.

Learning Objectives

In order to successfully complete this portion of the examination, you should be able to answer questions related to:

1. Obtaining internal and external information that explain the purpose of the organization and the environment within which it operates,
2. Analyzing operations by validating and comparing actual operations with the intended business model and strategy, and
3. Assessing organizational resilience.

Task Details

Obtain Internal Organization Information
To study how an organization functions, a risk professional must obtain reliable and valid information from internal and external sources. Two valuable sources of internal information come from documents and stakeholder interviews. Reports and documents organized by department or business unit are a good starting point to learn about organizational structure, process, and performance. Examples include reports from finance, operations, human resources, legal, and internal audit. Meeting with internal stakeholders and making site visits, if applicable, provides additional detail not captured in formal reports.

Obtain External Organization Information
External sources of information come from market analyses, regulation, and industry specific publications that interpret the effects of macro-economic forces that influence the strategic direction of the organization. As with internal sources of information, interviews with key external stakeholders and third-party site visits, if applicable, will provide valuable information for analysis. One of the more important outcomes of data collection from external sources of information is that which supports benchmarking analysis.

A successful risk management professional will be able to use not only his or her business acumen to find valuable documents but also utilize communication and research skills to collect information and apply lateral thinking to identify less obvious sources of information that will result in better analytical and risk strategy design outcomes.

Conduct Internal Analyses on the Organization
Once information of sufficient quality and quantity has been collected by the risk professional, the next step is to identify connections, whether strong or weak, between organizational objectives and risk philosophy. Prior to any meaningful analysis, information needs to be consolidated and organized. The risk professional collects and reads or listens to various reports to organize, synthesize, and prioritize information based on relevance to organizational objectives and their corresponding strengths and weaknesses. For example, in a heavily regulated industry, a risk management professional likely would pay close attention to material that focuses on risk associated with regulatory requirements and compliance.

Analyzing operations is like an internal due diligence process. A risk management professional utilizes active listening, interviewing, and communication skills to validate the organizational model. Specifically, information and behavior are compared to organizational culture, and alignment or potential disconnects are documented. Identifying how behaviors are rewarded can help align risk-taking decisions (e.g., sales force) with those bearing the risk (e.g., operations). Validation

also extends to a comparison of information and behavior as they relate to organizational strategy and the organization's attitudes toward uncertainties. For example, over-managed risks may come to light that initially may seem like a poor use of resources. However, after learning that the organization's tolerance for the risk is extremely low because it could destroy the value of the entire organization if managed incorrectly, the perceived "over-management" is deemed acceptable given the context of the organization's appetite and tolerance for risk.

Understanding an organization's value chains is an important outcome from analyzing the organizational model because they are inextricably linked to competitive advantage. A value chain is "a general framework for thinking strategically about the activities involved in any business and assessing their relative cost and role in differentiation. The difference between value, that is, what buyers are willing to pay for a product or a service, and the cost of performing the activities in creating it, determines profits."[3] Competitive pressure and the requirement to generate profit apply to any organization that intends to maintain its long-term viability and resilience. For example, a local non-profit organization that provides educational and support services to developmentally disabled children will have a different value chain than a multinational for-profit company that mines and sells minerals. Regardless, understanding an organization's value chain includes identification of:

- Series of business processes and steps that follow each other in succession intended to result in value creation for the organization.
- Resources within value chains.
- Key inputs and outputs of value chains.
- Differentiators within an organization compared to peers, and
- Influential macroeconomic factors that impact competitiveness and profitability.

Value chain analysis identifies areas for improvement, and the activities that provide the most value to customers and therefore the organization as a whole. Eliminating inefficient activities speeds up production, deliveries, improves competitive advantage, and increases the positive difference between revenues and expenses. Revenues are defined as revenues in for-profit organizations, donations in nonprofit organizations, and funding in governmental agencies. The difference between revenues and expenses is referred to as profit margin in for-profit entities, sustainability in nonprofits, and surplus in governmental agencies.

By identifying the activities and processes that create and sustain value for an organization, a risk professional is well positioned to develop risk strategies to minimize loss and maximize gain.

Another fundamental competency is the ability to benchmark an organization against competitors. Benchmarking involves measuring the performance of an organization against external standards of reference that frequently come from similar organizations doing similar things. A risk management professional utilizes research skills to identify peers and common practices. Often, this involves an analysis of the industry sector and relevant market segments. One's own organization may be ranked against peers based on deviations from value, either positive or negative. Frequently, external analysts research and compare risk factors noted in competitors' financial reports as well as those of industry partners in order to support investment decisions. When performed against external competitors or industry standards, benchmarking identifies strengths and weaknesses of the organization as well as areas where risk management can contribute to maximizing strengths and minimizing weaknesses. Combined with value chain analysis, benchmarking sets the stage for assessing organizational resilience.

Assess Organizational Resilience

There are two dimensions to organizational resilience. First is the traditional approach to hazard-based risk management such as business continuity planning, disaster preparedness, and crisis response. Second is the strategic approach of adaptation to chronic stresses and adapting to emerging forces in order to remain viable. ISO defines resilience as "the ability of an organization to absorb and adapt in a changing environment to enable it to deliver its objectives and to survive and prosper."[4] There is also a distinction in the literature between planned resilience and adaptive resilience where the former is based on historical events that can be predicted with varying degrees of accuracy and the latter is based on emerging events and trends that are less predictable.[5] Strategic risk management is a business discipline that drives deliberation and action regarding uncertainties and untapped opportunities that affect an organization's strategy and strategy execution. SRM offers an elegant approach to combining enterprise risk management with forward looking strategic methodologies to support the assessment of organizational resilience and identification of organizational uncertainties.

Assessing resilience begins with a comparison of existing capabilities and characteristics to those that are required, and then identifies shortcomings that need to be addressed. In the planned resilience space, mature business continuity programs utilize at least three methods that support resiliency gap analysis: business impact analyses, threat and risk analysis, and scenario planning. For example, the Threat and Hazard Identification and Risk Assessment methodology recommended by the United States Federal Government identifies capability targets, estimated current capabilities, and calculates gaps that may or may not be filled depending on risk tolerance, funding, and resource allocation constraints.[6]

In the adaptive resilience space, mature strategic risk management programs blend reactive traditional risk methodologies with forward looking strategic risk methodologies. Strengths, weaknesses, opportunities, and threats (SWOT) analysis is a methodology that represents a combination of planned and adaptive resilience. Identification of internal weaknesses and external threats support planned resilience. Identification of internal strengths and external opportunities supports adaptive resilience. The approach supports assessing organizational resilience because it offers an efficient way to collect information about both aspects of resilience and is easier to aggregate and share in reports that will later inform risk strategy design and implementation.

Risk professionals bring a valuable skill set to the planning process in an organization by identifying assumptions and bias within the organizational model. An assumption is something that is taken for granted. Sometimes organizational leaders may take for granted the existence of robust risk treatments and mitigations. Other times they may pursue new initiatives without thinking through the risk associated with the endeavor. Accurate assessments of organizational resilience are improved when risk professionals identify situations where risk treatments are lacking, or new risk has been taken on without an understanding of the solutions needed to effectively manage it. For example, when expanding production or sales to new markets and geographies, organizations may take for granted that the risk treatments developed in one area apply to others.

Decision makers are frequently influenced by bias as well. Bias is an unreasoned or preconceived feeling or opinion that influences behavior. Perceptual biases in decision making are difficult to recognize and frequently have a negative influence on outcomes. For example, an organization may feel like it is possible to achieve more than they can do in a certain amount of time. This is known as the planning fallacy. Assessing resilience of an organization is more complete when it incorporates methods to identify, document, and communicate the presence and impact of bias.

An important role of a risk professional is to collaboratively highlight strategic risks during the planning process and challenge the assumptions and logic underlying the cross-functional decisions to enable decision-makers to better plan for uncertainties in achieving the organization's mission, goals, and objectives.

Ultimately, the process of assessing organizational resilience results in the identification of uncertainties that could have the greatest impact–either negatively as obstacles or positively as accelerators- on achieving organizational objectives. Internal weaknesses are ranked based on their seriousness and relative importance to performance, and external threats are ranked based on likelihood and severity of occurrence. Internal strengths are ranked based on quality and relative importance to performance, and external opportunities are ranked based on ease of implementation and expected return. A careful review of key external drivers such as political, economic, social, technological, environmental, and legal drivers (PESTEL analysis) also provides valuable insights regarding uncertainties that could impact strategic direction of the organization.

A risk management professional needs to be assertive and inquisitive as uncertainties are documented and look for key assumptions and possible bias built into the organizational model that may not be explicitly understood. Developing a deep understanding of the organizational model is foundational for designing strategies for managing risk that should align with strategic objectives of the enterprise. Moreover, it should support the identification of specific contributions that risk management process can make to supporting organizational objectives.

After answering some sample questions and doing the self-assessment for the first domain, we will turn our attention to risk strategy design aspects of the RIMS-CRMP curriculum.

---

[3] Porter, M. E. (2008) Competitive Advantage: Creating and Sustaining Superior Performance. Simon and Shuster ebook.

[4] International Organization for Standardization. (2017). Security and resilience—Organizational resilience—Principles and attributes (ISO Standard No. 22316:2017).

[5] Barasa, E., Mbau, R., & Gilson, L. (2018). What Is Resilience and How Can It Be Nurtured? A Systematic Review of Empirical Literature on Organizational Resilience. International Journal of Health Policy and Management, 7(6), 491–503. https://doi.org/10.15171/ijhpm.2018.06

[6] United States Department of Homeland Security. (2018) Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Guide. https://www.fema.gov/sites/default/files/2020-04/CPG201Final20180525.pdf

Sample Exam Questions

1. A business model is a set of assumptions about the _____ .
   A. financial stability of an organization
   B. organizational structure of a business
   C. products and services' past performance
   D. way an organization creates value

2. What two analytical tools are particularly useful in analyzing the business model?
   A. Key performance indicators and total cost of risk
   B. Key risk indicators and gap analysis
   C. Pareto analysis and root cause analysis
   D. Value chain analysis and benchmarking

3. Risk management professionals conduct supply-chain analyses to identify _____ .
   A. contingent business interruption coverage
   B. customer technology needs
   C. international regulatory requirements
   D. potential vulnerabilities to the organization

4. Which activity does the risk management professional perform immediately after obtaining internal and external information about the organization?
   A. analyze the information
   B. organize the information
   C. prioritize the information
   D. report the information

5. Which risk identification and analysis technique should a risk management professional use in order to gather information from multiple departments in a brainstorming session that helps to identify shared risks within an organization?
   A. checklists
   B. flowcharts
   C. workshops
   D. questionnaires

6. When analyzing an organization's value chain, which of the following would be considered a primary activity?
   A. technological development
   B. human resources management
   C. infrastructure management
   D. outbound logistics

Self-Assessment of Content Areas

After you read the Analyzing the Organizational Model section and answer the practice questions, please rate your understanding and comfort level with each task from the first domain in Appendix A.

Domain 2: Designing Organizational Risk Strategies

The second RIMS-CRMP domain addresses the design of organizational risk strategies based on the business model of the organization. After completing organizational analysis that identifies how the entity generates profit, remains sustainable, or creates surplus, the risk professional turns his or her attention to the risk strategy design characteristics that will best support performance within the organization.

Learning Objectives

In order to successfully complete this portion of the examination, you should be able to answer questions related to:

1. Determining risk appetite and tolerance.
2. Developing risk strategy approaches.
3. Defining organizational risk competency and capabilities.
4. Designing risk management frameworks.
5. Obtaining organizational support for risk strategy.
6. Designing implementation plans.
7. Developing risk communication plans.

Task Detail

Determining Risk Appetite and Tolerance

Appetite means to desire greatly, long for, or seek after something, and tolerance is "the action or practice of enduring or sustaining pain or hardship."[7] Before reviewing definitions of risk appetite and tolerance, it is important to remember their metaphorical origins. For example, the RIMS definition of **risk appetite** is the total exposed amount that an organization wishes to undertake on the basis of risk-return trade-offs for one or more desired and expected outcomes; and its definition for **risk tolerance** is the amount of uncertainty an organization is prepared to accept in total or more narrowly within a certain business unit, a particular risk category or for a specific initiative (RIMS 2012). Although other definitions have variations in word choice, the idea of greatly desiring a reward while being intensely cognizant of the potential pain associated with seeking that reward helps establish thematic consistency regardless of the specific definitions utilized. Finally, risk appetite and tolerance exist simultaneously. Therefore, sometimes the terms are utilized to define each other. For example, in 2008 the BS31100 definition for risk appetite was "the amount and type of risk than an organization is prepared to seek, accept or *tolerate*" (emphasis added). Keeping these basic ideas in mind while beginning the design phase of risk management strategies will help maintain a coherent approach.

Clearly and accurately determining ownership of risk appetite and tolerance is important when designing organizational risk strategies because it helps create the aggregated risk philosophy of the organization. Risk taking is done by individuals at every level within an organization, and depending on the individual's position, risk appetite and tolerance may vary significantly. Think, for example, about the difference between highest level executive within an organization and the individual responsible for accounting, typically a controller. The former almost always has a higher risk appetite than the latter, and a more strategic mindset.

Clear ownership also supports validation of risk philosophy and the risk-taking culture of the organization. After careful scrutiny, the organization may determine that it is able to take on more risk in pursuit of objectives. Alternatively, an organization may choose to take on less risk as it identifies conflicts between those who are hungry for rewards but have little or no connection to the pain associated with the pursuit of those rewards. At the design stage, the emphasis is on defining risk taking culture in order to select and design a strategy that best fits the organization's overall mindset about risk.

Preliminary work done in the first domain of consolidating organizational information based on categories of risk naturally extends to the definition of parameters around risk taking behavior. As mentioned above, individuals take specific decisions about risk. As those decisions are aggregated by department or division, and ultimately aggregated at a portfolio level, determining categories and taxonomies of risk and opportunity will help build a coherent risk strategy approach.

[7] Murray, J. A. H. (1971). The Compact Edition of the Oxford English Dictionary (2 Volume Set) (18th Printing). Oxford University Press.

Determining risk appetite and tolerance also addresses the definition of metrics around risk taking behavior. For example, for a hazard-based risks, a common method for expressing risk appetite is to set a boundary on a probability and impact grid. These boundaries have direct implications on the purchase of insurance and determination of deductibles. For strategic-based initiatives, tolerance for loss can be based on capital measures and balance sheet expressions. For example, before proceeding with a strategic initiative, the organization may set a decision rule to only proceed if the probability of loss is not expected to exceed a certain percentage threshold.

The final aspect of determining risk appetite and tolerance that has a strong bearing on the remainder of the design phase is clear communication and understanding of risk philosophy. Internally, clear risk appetite and tolerance statements are the most critical inputs into the methodology of assessing risk and developing solutions to manage risk. Externally, well-articulated risk philosophy statements provide stakeholders peace of mind in knowing the organization has made good faith efforts to maintain its profitability and stability.

Developing Risk Strategy Approaches
Based on the organizational model and risk management needs, a risk management professional uses collective research to design a fit-for-purpose risk management strategy. The focus is on selecting risk management approaches that are most appropriate for the organization and its purpose, governance, strategy, objectives, operations, and decision-making style. Two of the most commonly used risk management guidance documents are the ISO 31000 international standard and the COSO ERM Framework. Risk management professionals should be familiar with both documents to determine how their guidance might be used in developing a customized risk strategy approach. Risk procedures and objectives may differ within an organization depending on its risk profile and risk attitude. When considering various risk strategy options, successful approaches generally are culturally appropriate and based on the needs of the organization. For example, highly regulated organizations with a deep foundation in analysis of quantitative metrics for decision-making will likely prefer statistical approaches for risk assessment and prioritization.

Developing tactics for integrating risk management techniques into organizational reporting and budgeting processes offers an important opportunity to seamlessly align risk management goals and objectives with those of the organization. Key enterprise planning functions, such as compliance, strategy, operations, internal audit, privacy and security, financial reporting, and risk disclosure represent integration opportunities. Determining risk management desired outcomes in light of the business needs generally reveals resource requirements and where internal support is needed. The reconciliation process at times results in risk strategies changing to accommodate the application of limited resources to desired outcomes. Aligning the selected risk strategy option with the organization's goals and objectives—at times, by answering "what outcome do we want to achieve?"—clarifies the value of the option when building a business case.

Defining Organizational Risk Competency and Capabilities
Once a risk strategy has been developed, a key consideration is whether an organization has the ability to successfully execute the approach. Ensuring that organizational risk management competencies support the risk strategy is another critical competency for a risk management professional. A review of existing capabilities based on a gap analysis will determine which capabilities are already in place. As gaps between risk management competency and risk strategy are identified, adequate resources should be either developed or acquired in order to meet risk management goals. For example, an organization may have strong risk identification processes in place because it religiously performs business risk assessments but lacks the ability to follow through on them and reinforce the importance of governance. Risk management professionals may look to different maturity models to help design a customizable approach for identifying gaps in capabilities, and either building or improving required risk competencies.

Defining the Risk Management Framework
Designing risk governance is a step that requires technical enterprise-wide risk management skills. Regardless of the framework selected -or that has been customized- one of the more important measures of effectiveness is integration. As noted in the ISO 31000 standard on risk management, "The effectiveness of risk management will depend on its integration into the governance of the organization, including decision-making." This requires commitment from stakeholders, particularly top management. Accountability for managing risk, at times referred to as risk ownership, is an important aspect of the technical design of risk governance. For example, there should be clear understanding of roles, responsibility, and accountability within the risk management governance structure.

Documentation of the risk management framework, standard, policies, procedures, and common vocabulary are incorporated into formal documents such as standard operating procedures (SOP) or manuals. Documentation of commitment to risk strategy from organizational leadership and risk owners is incorporated into the same SOPs or manuals in addition to other applicable governance documents related to the organization as a whole.

Obtaining Organizational Support for Risk Strategy
The next step in the design phase is to develop a value-based business case for the recommended risk strategy. The goal is to obtain commitment from leadership of the organization for the purpose, scope, accountability, responsibility, and resources to implement risk management strategy. Clear, compelling, and concise messages regarding the value expected to be gained from the risk strategy work well.

Value-based messages may be:

- Specific, such as identifying positive outcomes on a project specific basis (e.g., as we expect a 10% increase in customers, assumptions that may change the outcome will be tested);
- More general (e.g., as we expect an increase in share price vis a vis both the market and our competitors of 10%, volatility will be monitored); or
- Process based (e.g., deviations from formally established risk appetite and tolerance will be monitored and justified).

Once the messages are constructed around tangible value-based goals and outcomes, the risk professional needs to involve key decision makers and influencers within the organization and preview the business plan with them. It is important to validate the plan with these key decision makers to ensure alignment of the risk strategy with organizational objectives.

Designing Implementation Plans
The main components of an implementation plan are similar to project plans for other major initiatives. As such, risk management professionals need to be competent in project management, be able to identify the scope of the risk management initiative, set priorities for implementation, and engage key internal and external stakeholders. As with other projects, the implementation plan should identify key milestones, associated deliverables, and resources needed. Identification of implicit and explicit assumptions built into the plan such as dependencies, prerequisites, risks, and constraints helps provide assurance in meeting milestones. A project risk management review is conducted and once authorized, the implementation plan should be monitored periodically.

Success measures are based on a solid understanding of organizational goals and objectives as they relate to internal and external benchmarks. Success measures of the risk strategy itself are an important component of the design stage. As risk – the effect of uncertainty on objectives – is part of every decision, how well an organization takes risk into account when making strategic, operational, and tactical decisions should be one of the measures of success in risk strategies. Success measures at times are expressed as key performance indica¬tors (KPIs) and key risk indicators (KRIs). KPIs are measures that demonstrate progress toward achieving goals and objectives, while KRIs measure uncertainty associated with the achievement of goals.

Developing Risk Communication Plans
An important competency for risk management professionals is the ability to create a communication plan. A communication strategy, or plan, is a document that expresses the goals and methods of an organization's risk management activities, including what an organization wishes to share with various audiences and which stakeholders the organization is trying to reach. The plan formally defines who should be given specific information, when that information should be delivered and what communication channels will be used to deliver the information. A risk communication strategy can be developed as a component of the implementation plan and as a part of an organization's overall communication strategy.

The domain of designing organizational risk competency is the second largest domain as measured by average exam items because effective implementation is supported by well-designed strategy. Risk professionals who spend the time and effort required to build a solid foundation during the design stage will be better positioned for successful implementation of risk strategies.

Sample Exam Questions

7. The organization's resources and internal support are _____ the risk management strategy.
   A. adjustable to match
   B. inputs in the development of
   C. metrics used to measure the value of
   D. outcomes of the development of

8. When defining the success measures for the organization's risk strategy, the risk management professional will include which of the following steps?
   A. a review of the goals and objectives of the risk strategy
   B. a selection of appropriate media for communicating the risk strategy
   C. an analysis of the organization's total cost of insurable risk
   D. the development of timelines for implementing the risk strategy

9. Which of the following BEST guides an organization's risk management decision-making process?
   A. risk financing opportunities
   B. risk retention levels
   C. risk strategy approach
   D. risk treatment options

10. An effective risk communication strategy requires the selection of appropriate _____ .
   A. coaches
   B. data points
   C. media channels
   D. metrics

Self-Assessment of Content Areas

After you read the Designing Organizational Risk Strategies section and answer the practice questions, please rate your understanding and comfort level with each task from the second domain in Appendix A.

Domain 3: Implementing Risk Process

The third domain of the RIMS-CRMP certification addresses competencies related to implementing risk process. The risk process domain utilizes the background work from the first domain and the design work from the second domain and puts them into practice. Of the five domains, implementing risk process has the highest chance of contributing to an exam question.

Learning Objectives

In order to successfully complete this portion of the examination, you should be able to answers questions related to:

1. Identifying scope, context, and criteria.
2. Identifying risks and opportunities.
3. Analyzing risk.
4. Evaluating risk.
5. Collaborating with stakeholders to identify risk solution options.
6. Monitoring risk.

Task Detail

Identifying Scope, Context, and Criteria
The first step of implementing risk process takes preliminary work done in the organizational analysis and design phases and operationalizes those aspects in order to support specific risk management tasks. For example, external context identifies where risk identification process should be directed to capture relevant risks and opportunities. Internal context identifies how risk strategy aligns with organizational risk philosophy, goals, and objectives.

Scoping risk process specifies who is responsible for the execution of risk management process, what data collection and analysis methodologies will be used, and how information will be aggregated and reported to stakeholders. For example, customized registers that capture risk classifications, ownership, position, solutions, and excepted outcome are finalized during the scoping stage.

Finally, criteria are operationalized to support clear and repeatable analysis based on calculations of risk levels, measurements of management effectiveness, and residual positions of risk that are monitored within established risk appetite and tolerance thresholds.

Identifying Risk and Opportunity
As objective facilitators, risk management professionals serve as consolidators to aggregate and synthesize data that enable people within an organization to make risk-informed decisions. The risk identification process is comprised of finding, recognizing, and recording risks and opportunities using a variety of methodologies. For example, if a SWOT analysis was utilized to identify obstacles and accelerators to the achievement of organizational goals, the same methodology can be incorporated into the risk identification process. Additional data collection methods that might be useful include stakeholder interviews, focus groups, incident details, claims, surveys, financial statements, document reviews, and benchmarking. As data are collected, results are validated and recorded, capturing both threats and opportunities.

Analyzing Identified Risk
Risk analysis is the process of characterizing and understanding the nature of risk and of considering the level of risk in the context of the organization's willingness to accept risk in pursuit of its objectives. Successful risk analysis solves an issue or informs a decision when the criteria that will be employed to support the analysis and subsequent evaluation are fit for the purpose. Methods for analysis may need to be qualitative, quantitative, or based on a hybrid approach.[8] Certain risks or opportunities may require multiple analytical techniques to provide assurance and validation in the process. Analysis criteria determine which analytical methods should be used. For example, focus groups create long transcripts of conversations that can be organized thematically and support content analysis. Alternatively, financial results can be measured against different independent variables by using statistical analysis, while survey results may benefit from a hybrid method where data are first organized qualitatively and then scaled for quantitative analysis. Regardless of approach, both pure and speculative risk can be analyzed depending on the objective, related criteria, and chosen analysis method.

[8] While knowledge about how to do calculations related to specific risk analysis techniques and mathematical calculations are not required for the RIMS-CRMP exam, candidates must be able to apply the recognize components of risk analysis, and understand how and when to utilize methods for effective risk analysis.

Evaluating Risk
Risk evaluation combines results from risk analysis with measures of risk appetite and tolerance levels to determine which risks are acceptable in their current position and which require different solutions. Establishing definitions of what is significant for an organization—either statistically or qualitatively—creates thresholds to determine if risk appetite or tolerance have been exceeded or have not yet been met. Determining whether or not a risk or opportunity is within established control limits for risk appetite and tolerance supports the creation of risk solutions because it addresses allocation of resources. For example, time and money dedicated to overmanaged risks may be reallocated to undermanaged risks. Similarly, opportunities to take on more risk may be justified in pursuit of more value creation.

Interpretation of results of risk analysis identifies interdependencies among and between risks, supports aggregation of risk at a portfolio level, and clarifies potential consequences to the business model. As with risk analysis, successful risk evaluation is based on determining appropriate evaluation criteria for the decision under consideration, as well as exploitation and modification alternatives that fit into the overall risk philosophy of the organization.

Collaborating with Stakeholders to Identify Risk Solution Options
A risk management professional must be competent as a strategic advisor, solutions advocate and collaboration facilitator in developing and applying solutions to manage uncertainty. Collaboration is a fundamental competency since successful solutions must be tied to business model drivers, objectives and those who have primary responsibilities for managing risk, at times referenced as "risk owners." Collaboration also helps identify interdependencies between different solutions, leverages solutions that manage multiple risks with the same treatment and identifies inefficiencies where the solution may create more risk that it manages. Risk solutions should focus clearly and concisely on expected outcomes and align action with governance accountabilities.

Monitoring Organizational Risk
A fundamental competency of risk management professionals is creating a process for monitoring risk based on the organization's needs. Understanding the organization's priorities for monitoring highlights resources that are needed for the risk solutions expected to create the most value. An integrated method of monitoring risks is through performance metrics as measures of deviations from expected outcomes to help a firm see how it is performing based on key performance indicators (KPIs). Monitoring key risk indicators (KRIs) that affect business objectives simultaneously allow an organization to act at an early stage of performance deviations. Establishing schedules within the normal business calendar provides the foundation for a continuous improvement process, which emphasizes measurement of performance against metrics and validates the performance of risk solutions. Developing risk reporting that both informs risk owners and communicates actionable information at various levels of the organization helps drive change by making groups accountable and responsible and can be used to conduct follow-up activities as required.

Implementing risk process provides detailed and actionable outputs that help risk professionals engage in meaningful conversations with stakeholders and risk owners about how to improve competency in risk management throughout the organization, the topic of the fourth module.

Sample Exam Questions

11. Which of the following is considered a risk analysis technique?
    A. budget allocation
    B. consensus building
    C. insurance placement
    D. Monte Carlo simulation

12. When an operational area develops a treatment for a critical risk, the risk management professional MUST _____ .

A. add the risk to the risk map

B. communicate the treatment plan directly with internal audit

C. evaluate the dollar savings associated with the treatment

D. evaluate the impact upon other areas

13. A risk management professional advises management on the status of key risks by _____ .

A. annually identifying the inventory of risks

B. providing information about competitors' risk management plan

C. providing insights into the changing characteristics of a risk

D. summarizing internal audit reports

14. STEEP is a method used for strategic planning. The acronym STEEP stands for _____ .

A. security, technical, emerging, external, profit

B. social, technological, economic, environmental, political

C. standard, technique, enterprise, environmental, process

D. social, theory, external, engaging, program

15. Once risks have been analyzed, the risk management professional should evaluate the risks against the risk _____ .

A. appetite

B. monitoring plan

C. treatment

D. underwriting criteria

Self-Assessment of Content Areas

After you read the Implementing Risk Process section and answer the practice questions, please rate your understanding and comfort level with each task from the third domain in Appendix A.

Domain 4: Developing Organizational Risk Competency

The fourth RIMS-CRMP domain deals with developing organizational risk competency and focuses on how the organization as a whole develops and acquires risk management competencies, continuously improves, and ultimately incorporates risk management into its daily processes.

Learning Objectives

In order to successfully complete this portion of the examination, you should be able to answer questions related to:

1. Engaging an organization's risk network.
2. Delivering risk management training.
3. Coaching an organization on the risk process and techniques.
4. Continuously improving risk management process.
5. Integrating risk management into day-to-day operations.

Task Detail

Engaging an Organization's Risk Network
Developing a risk network promotes greater consistency in approach and capabilities for risk management activities throughout an organization. Exploring and respecting the risk management activities of each functional area allows a risk management professional to implement an approach that considers the risks and risk management practices of the organization as a whole. A key consideration in a successful exchange is the collaborative relationship among risk management professionals, the risk network, and others within the organization. A risk management professional should take the time to build relationships with influential executives to determine their views on how risk management can benefit the organization over time. Empathy and listening skills are important in understanding each person's concerns and being clear on what executives would like the organization to achieve. Risk management professionals should be seen as allies who support the organization in reaching its goals and objectives.

Delivering Risk Management Training
Executives consistently cite formalization of risk management training and education across the organization as a top focus area for developing organizational risk management capabilities in surveys that Marsh and RIMS conduct annually. Risk management training should align to specific business goals by determining the learning activities needed to reach performance goals through a training needs assessment, or gap analysis. Gap analysis seeks to answer the questions: "where are we?"—the current state and "where do we want to be?"—the desired future state. The results of this comparison, or gap analysis, determine the training content that needs to be provided to various audiences within the organization. Selection of communication channels is just as important as content. For example, depending on organizational culture and structure, face-to-face communication may be reserved for complex concepts, while the use of social media-based platforms may be more appropriate for updates.

Coaching an Organization on the Risk Process and Techniques
While training may be a one-time or periodic occurrence, risk coaching occurs on an ongoing basis. In some situations, formal risk management training is not supported or even possible, perhaps due to time and funding constraints. In these cases, risk management coaching becomes the main way to build organizational competencies. The term coaching typically refers to methods of helping others to improve, develop, learn new skills, find success, achieve aims, and to manage change and challenges. In organizational settings, coaching is the practice of providing support and advice to an individual or group in order to help them recognize ways in which they can improve their competencies and effectiveness. Risk management coaching involves providing guidance and support on becoming more proficient in using risk management process and techniques for problem solving in various environments. Coaching differs from training in style, approach, and structure.

Continuously Improving the Risk Management Process
Continuous improvement is an ongoing effort to improve products, services, or processes within an organization, and can be either informal (e.g., checklist) or more formal (such as using a plan-do-check-act methodology). An important aspect of organizational risk competency is adaptation through the process of continuous improvement. The process begins by identifying aspects of the risk process that need improving and then collaborating with other key stakeholders to develop alternative approaches. Alternatives should be validated with key stakeholders and those responsible for managing risk

before a new approach is chosen and implemented. Finally, the results of a new option should be monitored and modified as needed through an iterative process. Maturity models are a recognized measurement tool for demonstrating development progress and for highlighting consistent outcomes across organizations. Maturity as used here refers to an evolution toward the desired risk management attributes and competency drivers.

Integrating Risk Management into Day-to-day Operations
One of the indicators of a mature risk management process within an organization is the extent to which risk management is integrated into decision making at multiple levels of the organization. A risk management professional, with deep knowledge of the organization, has many opportunities to engage, influence, and build organizational competencies in risk management in various environments where decisions are being made. Opportunities could be in areas as diverse as innovation labs, research and development, customer relations, and day-to-day operations. Risk assessments are the most obvious examples of full integration. Strategic risk assessments focus on the broader deliberation and actions regarding uncertainties and untapped opportunities that affect an organization's planned strategy and strategy execution, such as growth (e.g., opening new markets) or contraction objectives (e.g., eliminating certain product or service lines). For example, has the organization built in a process to explicitly ask and answer risk-based questions about opportunities and threats regarding organizational objectives? Operational risk assessments may be limited to uncertainties associated with existing operations and plans—the assets, processes, people, and systems in place—in order to deliver a particular outcome, such as planned earnings.

Determining how alignment is measured between risk management methods and business outcomes strengthens integration. Project risk assessments typically are used to assess uncertainties and potential consequences related to expected outcomes of a particular project or initiative, such as delivering the project within the planned time, budget, and scope. Employees who understand their respective roles for managing risk that they can affect, and for raising awareness of risk they do not directly manage, accelerate integration.

An organization that has successfully integrated risk management into daily operations is well positioned to improve decision making as well. The final domain focuses on the contributions that risk management makes to supporting risk and resilience decisions.

Sample Exam Questions

16. After validating the training curricula, a risk management professional
    A. develops training
    B. develops and schedules training
    C. matches training to audience
    D. schedules and conducts training

17. What can a risk management professional recommend to management to protect an organization's critical infrastructure from a cyber attack?
    A. implement password protocols
    B. buy a tower of cyber liability insurance
    C. ensure employees do not post on social media
    D. monitor employees use of the internet

18. Risk tolerance is defined as the _____ .
    A. amount of uncertainty that an organization is prepared to accept
    B. desired level of risk that an organization believes is optimal to achieve its goals
    C. amount of risk that an organization can actually assume
    D. norms and traditions of the individuals of an organization and how they act on risk

Self-Assessment of Content Areas

After you read the Developing Organizational Risk Competency section and answer the practice questions, please rate your understanding and comfort level with each task from the fourth domain in Appendix A.

Domain 5: Supporting Decision Making

The final domain of the RIMS-CRMP deals with supporting decision making. With the successful establishment of risk process based on thorough organizational analysis and dedication to proper design, an organization can focus on value creation through improving decision making based on risk management tools and techniques.

Learning Objectives

In order to successfully complete this portion of the examination, you should be able to answer questions related to:

1. Influencing risk-based decision making.
2. Facilitating risk discussions.
3. Advise on risk and resilience decisions.

Task Detail

Influencing Risk-Based Decision Making
People throughout an organization make decisions every day. Some decisions are strategic and complex. Others are significant but less complex. Most are simple and frequent. Risk management is most effective when embedded into both routine and strategic decisions. Objectives and decision timelines drive the use of specific types of risk assessments - and analysis techniques - for different situations, the issues under consideration, and the type of decision being made. Therefore, a key competency for a risk management professional is the ability to incorporate risk management into decision making throughout an organization: listening skills, coaching and adeptness as a facilitator all come into play. While a risk management professional may not have formal training in decision sciences, understanding decision-making stages helps determine at what point he or she can influence a decision: 1) a pre-decision stage in which decisions have yet to be made, 2) an active decision stage in which decisions are in the process of being made, and 3) a post-decision stage in which decisions have already been made.

Identifying which decisions within each stage have the greatest impact on the business model and success of the objectives is also important. For example, a risk management professional may choose to emphasize high-impact decisions in the pre-decision category in order to minimize as much downside risk as possible and maximize as much gain as possible.

Other considerations are to identify who the actual decision makers are and to determine if there is a difference between the actual decision maker and the person accountable for the decision. Understanding risk-taking attitudes at each of the stages is also important.

The farther along people are in a decision-making stage about a strategic initiative, the less likely they might be to raise concerns regarding threats to the success of an initiative. Openly considering risk at each stage improves the odds that beneficial course corrections will be made to increase the odds of success.

For a risk management professional, understanding the components of quality decision-making is as important as understanding decision-making stages. Working with those who are engaged in the discussion (e.g., decision makers, accountable individuals, or impacted stakeholders) requires knowledge of the organization, how quality decisions are made, negotiation and leadership skills. Risk management professionals can assume a number of different roles in decision discussions such as: strategic advisor, observer, coordinator, or facilitator. As a facilitator, a risk management professional encourages participants to share relevant and reliable information by guiding a vigorous conversation. A facilitator has a responsibility to provide the team with updates on changes in the organization—whether those changes are operational or strategic—as well as emerging trends. In this role, a risk management professional should query and challenge what is said in order to fully develop a concept or issue and explore risk from multiple perspectives. Decisions made in one part of an organization may have ramifications in other areas. For example, launching a new product or service may affect the organization's ability to meet other customer needs. Successful risk discussions should draw out opportunities and alternatives, as well as uncertainties associated with potential outcomes of decisions. The goal is to confirm that the decision-makers take known and potential risk into consideration. Emphasis should be on transparency and consensus building concerning risk when taking decisions. If transparency becomes an issue or if consensus is unattainable, a process should be in place to escalate the discussion accordingly.

Advising on Risk and Resilience Decisions
As an organization manages risk on an integrated basis supported by project specific analysis, an important competency of a risk management professional is to provide insights that others may not readily recognize. Establishing a reputation as a

credible advisor on risk management and resilience enables risk management professionals to counsel other leaders within the organization (e.g., strategists, operations heads, or owners of initiatives), offering insights into risks affecting overall organizational performance.

With continuous monitoring and environmental scanning in place, risk owners identify new, changing, and emerging risks and opportunities. For example, risks may emerge that increase uncertainty around the achievement of organizational objectives. Additionally, untapped opportunities may emerge that—when acted upon—improve the organization's ability to adapt to change and absorb shocks. In order to advise on potential new options to respond to emerging risk, the same methodologies developed in the stage of implementing risk process are applied. The approach contributes to discussions about emerging threats to resilience with operational leaders, as much as it contributes to discussions about changes that could impact the stability and coherence of the organization with strategic leaders. Recommendations of new solutions benefit from existing process that ensures adequate monitoring and reviewing of the expected improvement in resilience of the organization.

The continuous identification of new, emerging, and changing risks impacts each of the four previous domains (see figure two). As an organization focuses on planned and adaptive resilience, fundamental characteristics of the organizational model may change because of large scale or systemic shocks in the operating environment of the organization. Changes to the design of organizational risk strategies may result as the organization learns from events and trends impacting performance. While implementation principles remain the same, there could be significant changes in the scope, context, and criteria of risk process based on emerging and disruptive movements in markets, customers, and competition. Finally, organizational risk competency may be challenged by emerging risk as well as requirements for new skills and abilities to manage risk effectively. With a dynamic process in place to ensure continuous improvement as well as adaptability, the chances of preserving long-term value of the organization improve.

Sample Exam Questions

19. What is the role of risk management in the strategic planning process?
    A. challenge the decisions made
    B. develop risk treatment plans
    C. draft the decisions to be made
    D. identify threats and opportunities

20. When measuring the financial effectiveness of an organization's risk management plan, the risk management professional should _____ .
    A. determine the overall cost of risk
    B. exclude risk financing costs
    C. involve the risk management committee
    D. determine the maximum level of uncertainty the organization can tolerate

21. How can an ERM heat map help to facilitate discussion for a risk committee?
    A. It provides a risk register for an organization to be able to review all risks.
    B. It identifies how mitigation efforts could affect frequency and severity of a risk.
    C. It provides a map for insurance companies to price an organization's premiums.
    D. It can help benchmark risks for comparison with others in the industry.

Self-Assessment of Content Areas

After you read the Supporting Decision Making section and answer the practice questions, please rate your understanding and comfort level with each task from the fifth domain in appendix A.

Appendix A

Self-Assessment Tool

Instructions

Rate your understanding and comfort level with each task after reading the domain section and attempting the practice questions. Score your understanding of each task based on a 5-point scale with 1 being the weakest and 5 being the strongest. Calculate the sum, then divide the total by the number of tasks. Finally, enter the quotient into the box for "Domain."

Example

		Self-Rank Score		
		Domain	Task	Note
A	**Analyzing the Organizational Model**	3.5		
1	Obtain internal organization information		3	
2	Obtain external organization information		5	
3	Conduct internal analyses on the organization		4	
4	Assess organizational resilience		2	
	Sum of self-scores by task		1	
	Divided by 4		/4	

Appendix A – continued

Self-Assessment Tool

	Self-Assessment of Duties and Tasks	Self-Rank Score: Domain	Task	Note
A	**Analyzing the Organizational Model**			
1	Obtain internal organization information			
2	Obtain external organization information			
3	Conduct internal analyses on the organization			
4	Assess organizational resilience			
	Sum of self-scores by task			
	Divided by 4			
B	**Designing Organizational Risk Strategies**			
1	Determine risk appetite and tolerance			
2	Develop risk strategy approach			
3	Define organizational risk competency and capabilities			
4	Define the risk management framework			
5	Obtain organizational support for risk strategy			
6	Design implementation plan			
7	Develop risk communication plan			
	Sum of self-scores by task			
	Divided by 7			
C	**Implementing Risk Process**			
1	Identify scope, context and criteria			
2	Identify risks and opportunities			
3	Analyze identified risk			
4	Evaluate risk			
5	Collaborate with stakeholders to identify risk solution options			
6	Monitor organizational risk			
	Sum of self-scores by task			
	Divided by 6			
D	**Developing Organizational Risk Competency**			
1	Engage organization's risk network			
2	Deliver risk training			
3	Coach organization on the risk process and techniques			
4	Continuously improve risk management process			
5	Integrate risk management into day-to-day operations			
	Sum of self-scores by task			
	Divided by 5			
E	**Supporting Decision Making**			
1	Influence risk-based decision making			
2	Advise on risk and resilience decisions			
	Sum of self-scores by task			
	Divided by 2			

Appendix A – continued

Self-Assessment Summary and Gap Analysis

Upon completion of each section of the self-assessment, you are now ready to perform a gap analysis to support allocation of exam preparation time. First, enter your self-rank score for each domain in the summary table below. Then, add them and divide by five in order to obtain a measure of your overall comfort level. To assign a ranking to each domain, compare your domain self-ranked score to the potential exam weight percentage. A rank of 1 identifies what you should study first.

		Self-Rank Score				
		Overall	Domain	Exam Weight	Rank	Note
	Domain					
A	Analyzing the Organizational Model			16%		
B	Designing Organizational Risk Strategies			26%		
C	Implementing Risk Process			32%		
D	Developing Organizational Risk Competency			16%		
E	Supporting Decision Making			10%		
	Sum of self-scores by task					
	Average (Divided by 5)					

Example

The hypothetical candidate below has the highest comfort level in implementing risk process, and therefore ranks the third domain as the last on which to spend time preparing. Although supporting decision making has the lowest comfort level, it is prioritized after developing organizational risk competency because the fourth domain represents a higher possibility of being on the exam.

		Self-Rank Score				
		Overall	Domain	Exam Weight	Rank	Note
	Domain	2.55				
A	Analyzing the Organizational Model		2.5	16%	3	
B	Designing Organizational Risk Strategies		3.25	26%	4	
C	Implementing Risk Process		4	32%	5	
D	Developing Organizational Risk Competency		2	16%	1	
E	Supporting Decision Making		1	10%	2	
	Sum of self-scores by task		12.75			
	Average (Divided by 5)		/ 5			

Glossary

Benchmarking: The process of measuring the performance of an organization against external standards of reference that frequently come from similar organizations doing similar things.

Corporate governance: The system of rules, practices, and processes by which a company is directed and controlled. (Investopedia http://www.investopedia.com/terms/c/corporategovernance.asp#ixzz4QO62g4aC)

Enterprise risk management: A strategic discipline that supports the achievement of an organization's objectives by addressing the full spectrum of its risk and managing the combined impact of those risks as an interrelated risk portfolio. (RIMS, 2010)

Gap analysis: Comparison of an existing process or procedure (current state-what is) to a desired, future state (what should be) in order to identify deficiencies or excesses in the existing process (what to consider). (ANSI/ASIS/RIMS Risk Assessment Standard RA.1-2015, p.45-46)

Key performance indicator (KPI): Measure(s) of deviations from expected outcomes to help a firm see how it is performing. (RIMS, Transitioning to ERM, 2014)

Key risk indicator (KRI): Leading indicator(s) of risk to business performance, giving early warning about potential risks. (RIMS, Transitioning to ERM, 2014).

Organizational Resilience: The ability of an organization to absorb and adapt in a changing environment to enable it to deliver its objectives and to survive and prosper.

PESTLE analysis: PESTLE is an acronym for Political, Economic, Social, Technological, Legal and Environmental and identifies the categories utilized to analyze internal and external environments. Other forms of the acronym include "PEST" and "PESTEL."

Risk: The effect of uncertainty on objectives. (ISO 31000:2018, Guide 73:2009)

Risk appetite: The total exposed amount that an organization wishes to undertake on the basis of risk-return trade-offs for one or more desired and expected outcomes (RIMS, Exploring Risk Appetite and Risk Tolerance, 2012).

Risk attitude: An organization's or individual's view/perspective of the perceived qualitative and quantitative value that may be gained in comparison to the related potential loss or losses. (RIMS, Exploring Risk Appetite and Risk Tolerance, 2012)

Risk culture: The beliefs, values, norms, and traditions of behavior of individuals and groups within an organization that determine the way in which they identify, understand, discuss, and act on the risk(s) the organization confronts and takes. (RIMS, Exploring Risk Appetite and Risk Tolerance, 2012)

Risk champion: Any person in an organization who is a leader and influences peers regarding the value that risk management adds to the organization.

Risk governance: Encompasses the oversight, practices and respective roles and responsibilities for risk within an organization's unique corporate governance.

Risk management: Coordinated activities to plan, direct, control and make decisions concerning the effects of uncertainty on objectives. (adapted from ISO guide 73:2009)

Risk owner: An individual accountable for the identification, assessment, treatment, and monitoring of risks in a specific environment. (Elliott, 2014, p. 3.5)

Risk portfolio: A broad collection and range of uncertainties that can affect an organization's future.

Risk tolerance: The amount of uncertainty an organization is prepared to accept in total or more narrowly within a certain business unit, a particular risk category or for a specific initiative. (RIMS, Exploring Risk Appetite and Risk Tolerance, 2012)

Root cause: Underlying or initiating risk source or driver that produces certain outcomes or changes the impact of an outcome or outcomes. Commonly used to describe the point in a chain of events or conditions where an intervention could reasonably be implemented to improve performance or prevent an undesirable outcome. (adapted from ANSI/ASIS/RIMS Risk Assessment Standard, RA.1-2015)

Root cause analysis: Multiple risk assessment techniques and approaches, at times applied in a series, which are designed to identify the underlying or initiating risk source(s) or driver(s). (ANSI/ASIS/RIMS Risk Assessment Standard, RA.1-2015. P. 93)

Strategic risk management (SRM): A business discipline that drives deliberation and action regarding uncertainties and untapped opportunities that affect an organization's strategy and strategy execution. (RIMS Strategic Risk Management Implementation Guide, 2012).

SWOT analysis: SWOT is an acronym for Strengths, Weaknesses, Opportunities, and Threats and is an analytical approach for environmental scanning that combines internal and external context with obstacles and accelerators to success in achieving objectives.

Value chain: A high-level model developed by Michael Porter used to describe the process by which businesses receive raw materials, add value to the raw materials through various processes to create a finished product, and then sell that end product to customers. (Investopedia http://www.investopedia.com/terms/v/valuechain.asp#ixzz4QO5T8TRD)

Value chain analysis: A strategy tool used to analyze internal firm activities. Its goal is to recognize which activities are the most valuable (i.e., are the source of cost or differentiation advantage) to the firm and which ones could be improved to provide competitive advantage. (Strategic Management Insight: www.strategicmanagementinsight.com/tools/value-chain-analysis)

Top 10 Exam References

1. Chapman, Robert. Simple Tools and Techniques for Enterprise Risk Management, 2nd ed., John Wiley & Sons, Ltd, London, 2011.

2. Elliott, Michael. Risk Management Principles and Practices, The Institutes, Malvern, PA.

3. Fraser, J. and Simkins, B.J. Enterprise Risk Management, 1st ed., John Wiley & Sons, Inc., Hoboken, NJ.

4. Gamble, John; Thompson Jr., Arthur; Peteraf, Margaret. Essentials of Strategic Management: The Quest for Competitive Advantage, 6th ed, 2019.

5. Hopkin, Paul. Fundamentals of Risk Management, 2018.

6. International Organization for Standardization. Risk Management — Guidelines (ISO Standard No. 31000:2018).

7. Moeller, Robert. COSO Enterprise Risk Management, John Wiley & Sons, Inc., Hoboken, NJ.

8. RIMS Executive Report, Exploring the Risk Committee Advantage, RIMS, New York, NY, 2015.

9. RIMS Executive Report, Transitioning to Enterprise Risk Management, RIMS, New York, NY, 2014.

10. Strategic Risk Management Development Council. RIMS Strategic Risk Management Implementation Guide, RIMS, New York, NY.

Practice Questions

22. A success criterion for a risk management program includes
    A. Risk accountability
    B. Dependencies
    C. Organizational structure
    D. Performance

23. Which of the following is the BEST example of a reason to revise a risk management program?
    A. A new exposure arises such as a new merger or acquisition
    B. Significant turnover within the risk management function
    C. New product offerings by the insurance industry
    D. A revision of a company's annual earnings forecast

24. A potential DISADVANTAGE of benchmarking is that it
    A. May limit the type of information obtained if it only considers organizations viewed as a direct competitor
    B. Focuses primarily on areas of overlap in product or services and does not consider areas in which organizations differ
    C. Focuses primarily on company best practices and cannot be used to identify areas for possible innovation
    D. Does not provide useful information about industry and market trends

25. Which industry environmental factors create uncertainty for an organization?
    A. Demand and competition
    B. Cultural factors
    C. Transportation and infrastructure
    D. Historical claims experiences

26. To increase the likelihood that a risk strategy approach will be adopted, it is important for a risk management professional to understand the organization's
    A. Governance
    B. Hierarchy
    C. Culture
    D. Profit margins

27. A risk management oversight body focuses on what quadrant of risk as aligning closest to its organization's ability to meet corporate objectives?
    A. Hazard
    B. Financial
    C. Strategic
    D. Operational

28. Risk Mapping is an effective visual tool employed by risk management professionals to
    A. Capture risk portfolio relative frequency and severity
    B. Define historical risk portfolio materiality thresholds
    C. Provide Monte Carlo Simulation inputs
    D. Confirm validity of loss triangles

29. When a line employee identifies a risk, to whom should the information first be reported to?
    A. Compliance Officer
    B. Operations Manager
    C. Risk Committee
    D. Risk Manager

30. The purpose of documenting business model uncertainties is to
    A. Prioritize the impact of residual risks
    B. Conduct a review of the enterprise risk management framework
    C. Disqualify a business case to support loss control measures
    D. Provide a tangible resource for the design of risk strategies

31. What is one KEY advantage that can be used to obtain organizational support for adopting an enterprise risk management strategy?
    A. Increased capital flows associated with increased risk controls
    B. Reduced scrutiny from management or oversight boards
    C. Improved effectiveness of safety and security practices
    D. Reduced governance costs through increased control efficiency

32. As the concept of organizational resilience evolves, what is ONE critical challenge to communicating and implementing a sustainable process?
    A. Economic cost of implementing a resilient program design
    B. Resilience across and between organizational cultures
    C. Market recognition of resilience program effectiveness
    D. Ensuring alignment between resilience program design and execution when needed

33. A risk management professional evaluates which type of key external force to gain insight about another company's strengths and weaknesses?
    A. Political
    B. Competitive
    C. Economic
    D. Technological

34. A timeline is included in the
    A. Risk implementation plan
    B. Risk governance structure
    C. Risk management framework
    D. Risk monitoring metrics

35. The three components that make up the risk assessment phase of the risk management process are
    A. Establishing the context, risk evaluation, and risk treatment
    B. Establishing the context, risk identification, and risk evaluation
    C. Risk identification, risk analysis, and risk evaluation
    D. Risk identification, risk analysis, and risk treatment

36. When working with risk owners to develop risk treatment, it is necessary to
    A. Consider risks equally
    B. Consider risk within the context of the business
    C. Generate a positive return on investment in the current year
    D. Seek approval from the Board of Directors

37. The risk management professional should prioritize information about the business model based on
    A. Industry trends
    B. Annual reports
    C. Analyst reviews
    D. Strategic objectives

38. When seeking to advise the organization on risks, the risk management professional should try to adopt what type of relationship model?
    A. Compliance
    B. Operational
    C. Partnership
    D. Sales

39. Which of the following would signal a potential change in an organization's risk context?
    A. The organization acquires a new business
    B. The organization changes insurance brokers
    C. The organization's board of directors reviews a compliance report
    D. The organization publishes its annual report

40. What is the FIRST step in delivering risk training?
    A. Developing training
    B. Identifying existing training
    C. Identifying training needs
    D. Scheduling training

41. The risk management professional can use various risk dimensions to analyze risks. These include impact, likelihood and
    A. Change in size
    B. Coefficient of reliability
    C. Collective opinion or team rating
    D. Speed of onset or velocity

42. Which type of risk management is the most influential in facilitating risk discussions on a board or similar organizational level?
    A. Integrated
    B. Enterprise
    C. Traditional
    D. Advanced

43. Which approach should be used to reduce the risk of perception bias when conducting a facilitate risk workshop?
    A. Working with managers
    B. Working with a diverse group
    C. Working with other risk management professionals
    D. Working with a large group

44. To gain greater insight on the effects of uncertainty on organizational objectives, the risk management professional
    A. Has a strong incentive to consult and communicate organizational risks
    B. Should consult with key risk stakeholders
    C. Should focus on identifiable risks
    D. Has a duty to inform when risks are outside of a risk tolerance

45. An effective way for a risk management professional to analyze operations of an organization is to form a
    A. Risk committee
    B. Captive insurance company
    C. Risk management department
    D. Template to gather information

46. Before a decision is made, which of the following issues should ALWAYS be escalated to higher level risk committees, management committees, or the Board?
    A. Those that are important but lack critical information
    B. Those that are overly complex and not well understood
    C. Those that exceed the authority of the intended decision maker or decision-making body
    D. Those that fall within the authority of the intended decision maker or decision-making body

Answer Key

Domain 1: Analyzing the Organizational Model

1. **D**

The business model represents the value an organization creates.

Reference: Gamble, John; Thompson Jr., Arthur; Peteraf, Margaret. Essentials of Strategic Management: The Quest for Competitive Advantage, 6th ed, 2019.

2. **D**

The risk management professional should utilize appropriate analytical tools for analyzing the business model.

Reference: Gamble, John; Thompson Jr., Arthur; Peteraf, Margaret. Essentials of Strategic Management: The Quest for Competitive Advantage, 6th ed, 2019.

3. **D**

The vulnerability of the supply-chain helps determine the organization's ability to meet performance objectives.

Reference: Gamble, John; Thompson Jr., Arthur; Peteraf, Margaret. Essentials of Strategic Management: The Quest for Competitive Advantage, 6th ed, 2019.

4. **B**

To properly perform due diligence, the risk management professional needs to know the order of processing the information. Information must be organized before it can be analyzed, prioritized, or reported.

Reference: Strategic Risk Management Development Council. RIMS Strategic Risk Management Implementation Guide, RIMS, New York, NY.

5. **C**

Workshops have an advantage in that they have a facilitator that can help to guide the discussion and identify information in this interactive format. Checklists, flowcharts, and questionnaires are less able to identify shared risks between departments as they are completed in a silo approach.

Reference: Elliott, Michael. Risk Assessment and Treatment, The Institutes, Malvern, PA.

6. **D**

Porter's value chain model considers the following to be primary activities: Inbound logistics, Operations, Outbound Logistics, Marketing and Sales, and Service.

Reference: Porter, Michael. Competitive Advantage, Free Press, New York, NY, 1985.

Domain 2: Designing Organizational Risk Strategies

7. **B**

The appropriate risk management strategy aligns with the organization's internal resources and support

Reference: Chapman, Robert. Simple Tools and Techniques for Enterprise Risk Management, 2nd ed., John Wiley & Sons, Ltd, London, 2011.

8. **A**

Success measures can only be defined if one understands the strategy's goals and objectives.

Reference: Moeller, Robert. COSO Enterprise Risk Management, John Wiley & Sons, Inc., Hoboken, NJ.

9. **C**

The design of the risk management framework should facilitate the integration of the risk management process into decision-making and the overall management of the organization.

Reference: International Organization for Standardization. Risk Management - Guidelines (ISO Standard No. 31000:2018).

10. **C**

Communicating with stakeholders is done via one of two channels, depending on whether the audience is internal or external.

Reference: Fraser, J. and Simkins, B.J., Enterprise Risk Management, 1st ed., John Wiley & Sons, Inc., Hoboken, NJ.

Domain 3: Implementing Risk Process

11. **D**

Insurance placement is considered risk treatment—not analysis.

Reference: Chapman, Robert. Simple Tools and Techniques for Enterprise Risk Management, 2nd ed., John Wiley & Sons, Ltd, London, 2011.

12. **D**

Operations and plans should be examined to ensure appropriate integration and coordination.

Reference: Fox, C. and Seigel, M., ANSI/ASIS/RIMS RA 1. Risk Assessment, ASIS & RIMS, New York, 2015.

13. **C**

Evaluating the inventory of risks and monitoring internal audit reports are risk identification activities, not advising on risk management.

Reference: Moeller, Robert. COSO Enterprise Risk Management, John Wiley & Sons, Inc., Hoboken, NJ.

14. **B**

STEEP is one traditional method used in strategic planning and has five sectors (Social, Technological, Economic, Environmental, Political).

Reference: Strategic Risk Management Development Council. RIMS Strategic Risk Management Implementation Guide, RIMS, New York, NY.

15. **A**

The criteria for assessing the acceptability or otherwise of risks is usually set prior to the evaluation commencing, and should reflect the organization's risk context, tolerance, appetite, and the views of stakeholders.

Reference: International Organization for Standardization. Risk Management - Guidelines (ISO Standard No. 31000:2018).

Domain 4: Developing Organizational Risk Competency

16. **D**

Thinking through a process: identify needs, develop, validate, schedule, and conduct.

Reference: International Organization for Standardization. Risk Management - Guidelines (ISO Standard No. 31000:2018).

17. **A**

There are many things that a risk management professional can recommend. Requirement of strong passwords and the necessity to change them on a periodic basis will help to protect the organization.

Reference: Cabrera, Ed, "Protecting Critical Infrastructure from Cyberattack", Risk Management Magazine, October 3, 2016.

18. **A**

Option B is defined as risk target; Option C is risk capacity; and Option D is the risk culture of an organization.

Reference: RIMS Executive Report, Exploring the Risk Committee Advantage, RIMS, New York, NY, 2015.

Domain 5: Supporting Decision Making

19. **D**

Of the response options available, D is the best choice.

Reference: Elliott, Michael. Risk Assessment and Treatment, The Institutes, Malvern, PA.

20. **A**

Determination of the COR is the primary measure used by many organizations to gauge effectiveness.

Reference: Elliott, Michael. Risk Financing, The Institutes, Malvern, PA.

21. **B**

When a heat map is used in workshops to assess the risks by individual managers, the discussions can be enhanced to see how risks in one part of the organization impacts another part of the organization. The resulting heat map can also be used to communicate the risk assessment to senior management, audit committees, and boards of directors. The heat map also enables a business conversation about mitigation alternatives.

Reference: Elliott, Michael. Risk Assessment and Treatment, The Institutes, Malvern, PA.

Practice Questions

22. **A**
23. **A**
24. **A**
25. **A**
26. **C**
27. **C**
28. **A**
29. **B**
30. **D**
31. **D**
32. **B**
33. **B**
34. **A**
35. **C**
36. **B**
37. **D**
38. **C**
39. **A**
40. **C**
41. **D**
42. **B**
43. **B**
44. **B**
45. **A**
46. **C**

Disclaimer

This guide is intended to provide only a general overview of the topics related to the RIMS-CRMP certification exam. This is not a complete analysis. The information provided is for general use only and is not intended to provide specific advice or recommendations, legal or otherwise, for any individual or organization. The information provided in this document is not mandatory to study nor does it guarantee a passing score on the RIMS-CRMP certification examination.

Contributors

Joseph A. Milan, PhD, ARM
Principal, JA Milan and Associates, LLC

Carol Fox, ARM
VP, Strategic Initiatives, RIMS, *the* risk management society®

Christine D. Niero, PhD
Vice President, Professional Certification and Client Development
Professional Testing, Inc.

Denise Osorio
Director of Certification Programs, RIMS, *the* risk management society®

SME Reviewers

Randy F. Jouben, CPCU, ARM, CBCP, MBCI
Executive Director, Risk Management and Compliance
College of Southern Maryland

Darius Delon, MBA, RIMS-CRMP, CCIB, FCIP
Principal, Riskmanagement101.ca

RIMS, the risk management society®

RIMS, the risk management society®, empowers risk professionals to make the world safer, more secure, and more sustainable. Through networking, professional development, certification, advocacy, and research, RIMS and its 80 chapters serves more than 200,000 risk practitioners and business leaders from over 75 countries. Founded in 1950, the Society publishes the award-winning Risk Management Magazine and produces RISKWORLD®, the largest annual gathering of global risk professionals. RIMS embraces diversity, equity, and inclusion and welcomes all risk professionals to connect and learn.

Version 7.0: Published April 2025

RIMS-CRMP-FED®

RIMS-Certified Risk Management Professional For Federal Government

RIMS-CRMP-FED Study Guide

Certification Programs

228 Park Ave S PMB 23312 New York, NY 10003-1502
(212) 286-9292 | RIMS-CRMP@RIMS.org
www.RIMS.org

RIMS® *the* risk management society

Table of Contents

Tables and Figures

Introduction

Those who qualify to take the RIMS-CRMP-FED examination have already met the eligibility requirements identified in the Candidate Handbook and passed the exam for the RIMS-CRMP.

The purpose of this section of the study guide is to support candidates taking the RIMS-CRMP-FED micro-credential examination. It is not intended to replace any textbook or other resources you need to prepare for the examination, and using this guide does not guarantee that you will pass the micro-credential examination.

The study guide is divided into two sections. The first section deals with the background of the RIMS-CRMP-FED micro-credential and provides guidance on the process of the micro-credential examination.

The second section summarizes three core competencies of a risk professional in the federal government of the United States:

1. Understanding the Federal Government Risk Management Environment
2. Risk Management Implementation in the Federal Government
3. Risk Management Reporting in the Federal Government

It then reviews each competency based on four of the same components that were utilized for the core RIMS-CRMP credential:

1. Learning objectives
2. Examples
3. Self-assessment of content areas
4. Sample exam questions

The study guide concludes with a glossary of terms and bibliography.

Section 1 — Background and Process

About the RIMS-CRMP-FED Micro-Credential

The RIMS-CRMP-FED is a micro-credential that was developed in cooperation with the Association for Federal Enterprise Risk Management (AFERM) and distinguishes the achievement of validated risk management competencies for an effective risk management professional in the federal government environment. Individuals who earn the RIMS-CRMP-FED have demonstrated their knowledge and competency in the area of risk management in the United States federal government, and are dedicated to upholding the same high standards of ethical and professional conduct that apply to the core RIMS-CRMP credential.

RIMS-CRMP-FEDs may use the credential to establish credibility within their organization and among risk management professionals. Adding the RIMS-CRMP-FED certification to your professional profile verifies that you have achieved a high level of expertise, education and experience required to successfully manage risk and support decision making in the federal government environment.

Strategies for Analysis of an Exam Question

Questions on the RIMS-CRMP-FED examination are based on the same structure and approach as the core exam (i.e., four-choice multiple- choice item type format). All questions and answers are referenced to an industry-accepted textbook or resource, and each question has been reviewed by a number of experienced professionals in the field who agree on the correct answer. In addition, a substantial amount of empirical data has been collected on each question to assure that it performs appropriately and effectively. The four answers presented may not agree with your individual interpretation of the material. Regardless, it will be necessary to choose one of the four answers provided as the best answer.

Test Preparation Strategies

The guidelines that apply to the core credential also apply to the micro-credential:

- **References provided throughout this review section do not constitute a required reading list, but rather are examples of acceptable sources for examination questions.**
- The important topics that candidates should study to successfully prepare for the examination are listed in the examination blueprint
  of core competencies.
- Learning objectives and examples provided in this study guide have been developed independently of the examination questions.

The micro-credential domain blueprint (see Table 1-FED on page 6) contains the major content areas on the exam, and the percentage of the exam each content area represents. Use the blueprint as a guide in identifying any content areas you need extra time and resources to prepare for, and ask yourself these questions.

- Which content areas represent the greatest number of test questions? The greater the number of possible questions on the exam, the more focus you need on these topics to prepare.
- How much time do you need to focus on these areas to prepare for the exam, versus other areas?
- How do your current knowledge and skills compare to the content areas of the exam? Are you strong in some, but weak on others? Making this assessment will help you allocate your study time.
- How much training or work have you done in the areas on the exam? If you have had extensive training and/or experience in a specific area, you may decide that your focus should be on the areas that are less familiar to you.

Your analysis of the content outline and your answers to the questions above will help you determine where you need to spend your study time. Eventually you will decide that you have studied all you can. Once you have reached this point, you should schedule an appointment to take the examination.

What to Expect at the Testing Center

As with the examination for the core credential, examinations for the micro-credential are administered by Pearson VUE. Therefore, all of the logistical considerations discussed above apply to the examination for the micro-credential as well. The main difference between the examinations is that the micro-credential test is shorter and is comprised of 50 questions with a 60-minute time limit.

Table 1-FED
RIMS-CRMP-FED Domains

Domain	Duties and Tasks	% Exam
A	**Understanding the Federal Government Risk Management Environment**	**40%**
	A.1 Identify sources of government information and reporting (e.g., GAO, OIG, Grantees)	
	A.2 Assess key stakeholders	
	A.3 Identify the relationship between risks and controls in the Federal government environment	
	A.4 Analyze Federal government risk controls and other risk management initiatives according to Federal government standards (e.g., OMB, GAO, DOD, NARA, NIST)	
	A.5 Identify Federal government reporting requirements	
	A.6 Distinguish between Federal government requirements	
B	**Risk Management Implementation in the Federal Government**	**40%**
	B.1 Communicate role and responsibilities within the Federal government ERM process	
	B.2 Coordinate and work with stakeholders and partners (e.g., oversight bodies, internal, external, public or private sector, Federal, State, Local, Tribal, Territorial)	
	B.3 Engage Federal Government risk networks	
	B.4 Develop two-way internal communication strategies on the Federal government ERM process	
	B.5 Align internal controls to balance risk and opportunities with Federal government risk tolerance	
	B.6 Implement risk controls and other risk management initiatives according to Federal government standards (e.g., OMB, GAO, DOD, NARA, NIST)	
C	**Risk Management Reporting in the Federal Government**	**20%**
	C.1 Prepare internal reports according to Federal government reporting requirements	
	C.2 Prepare external reports according to Federal government reporting requirements	
	C.3 Report on the effectiveness of Federal government risk control according to standards (e.g., OMB, GAO, DOD, NARA, NIST)	
	C.4 Provide advice to federal officials on risk reporting and responses	
	Total	**100%**

Section 2 — Exam Blueprint and Review Components

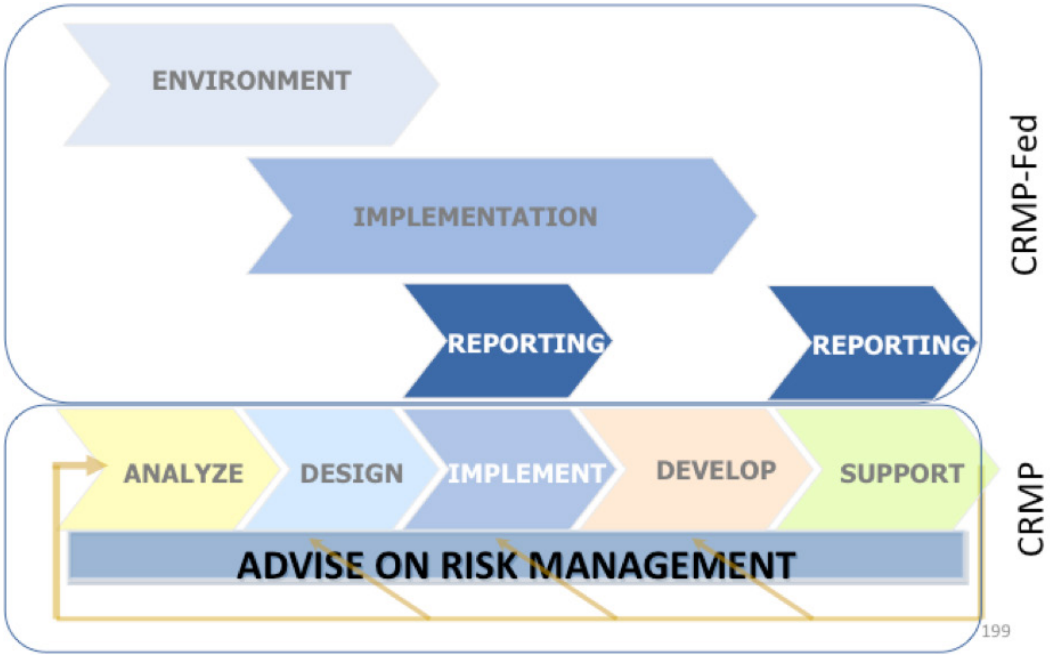
Examination Blueprint

The core competency areas are depicted in Table 1-FED as the key duties and tasks associated with each domain. The column on the right side of the table shows the percentage weight each domain has within the overall exam. The weighting will help you prioritize study time and identify opportunities for personal improvement.

The first micro-credential domain, "Understanding the Federal Government Risk Management Environment," provides detail that relates to the core RIMS-CRMP domains of "Analyzing the Business Model" and "Designing Organizational Risk Strategies." The second micro-credential domain, "Risk Management Implementation in the Federal Government," provides detail that relates to the core RIMS-CRMP domains of "Designing Organizational Risk Strategies," "Implementing the Risk Process" and "Developing Organizational Risk Competency."

The third micro-credential domain, "Risk Management Reporting in the Federal Government", provides detail that relates to the core RIMS-CRMP domains of "Implementing the Risk Process" and "Supporting Decision-Making." Figure 1-FED is a graphical representation of the relationship between the micro-credential domains and those of the core RIMS-CRMP credential.

Figure 1-FED
Comparison of RIMS-CRMP-FED Domains to RIMS-CRMP Domains



Review Components

Each domain is broken down into four areas to aid the studying process:

1. **Learning objectives** provide more detail around the tasks identified in the exam blueprint.

2. **Examples** provide more detail in the form of definitions and illustrations.

3. **Self-assessment of content areas** offers you an opportunity to self-rate your competency in each domain area generally and each content area more specifically. Appendix B has a clean copy of the self-assessment worksheet that can be used multiple times to track your progress and perform comparisons.

4. **Sample exam questions** give a real-life look at how questions are worded and show the source that supports the answer to the question.

Section 3 — Review

Domain 1: Understanding the Federal Government Risk Management Environment

The first competency domain in the RIMS-CRMP-FED curriculum addresses some of the unique environmental and contextual considerations relevant to the federal government.

Learning Objectives

To successfully complete this portion of the examination, the certification candidate should be able to:

1. Identify sources of government information and reporting (e.g., GAO, OIG, Grantees).
2. Assess key stakeholders within the federal government.
3. Identify the relationship between risks and controls in the federal government environment.
4. Analyze federal government risk controls and other risk management initiatives according to federal government standards (e.g., OMB, GAO, DOD, NARA, NIST).
5. Identify federal government reporting requirements.
6. Distinguish between federal government requirements.

Examples

Sources of government information and reporting. The first domain of the core credential blueprint discussed how to analyze the business model of an organization and identify sources of information that explain the purpose of an organization and describe the environment within which it operates. Unique considerations related to the federal government that should be included in this analysis include
identifying federal government specific sources of information and reporting. Given the importance of internal controls in the federal government, sources of information frequently come from activities that support internal controls assessments. For example, internal management reviews that focus on financial systems, cyber security and performance management provide valuable insights into risk management governance, framework and process. Additionally, external reports such as Office of Inspectors General (OIG) Management Challenges and Government Accountability (GAO) High Risk Reports can serve as measures of severity associated with certain key risks faced by a federal agency.

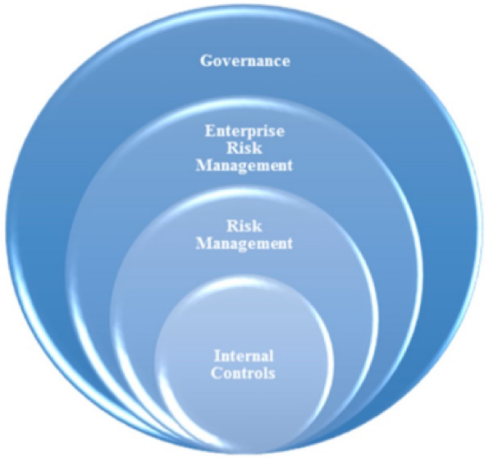
Assess key stakeholders within the federal government. The federal government environment is also unique from a stakeholder analysis standpoint because the overlap between internal and external stakeholders may be more common than the private sector. Certain stakeholders are readily classifiable as external (e.g., lobbyists) and internal (e.g., employees of the agency). However, often a stakeholder such as the OIG or other federal agencies are a hybrid and simultaneously represent internal and external perspectives and pressures. Specifically, stakeholders will have expectations about risk appetite and tolerance for the agency and, depending on the stakeholder's degree of influence, may have a significant impact on how the agency manages risk and its business processes on a day-to-day basis. A clear understanding of who the relevant stakeholders are for a federal agency and what their expectations are regarding risk appetite and tolerance will help set the foundation for effective enterprise risk management (ERM).

For ERM in the federal government, risk appetite "is the broad-based amount of risk an organization is willing to accept in pursuit of its mission/vision. It is established by the organization's most senior level leadership and serves as the guidepost to set strategy and select objectives." Risk tolerance "is the acceptable level of variance in performance relative to the achievement of objectives. It is generally established at the program, objective or component level. In setting risk tolerance levels, management considers the relative importance of the related objectives and aligns risk tolerance with risk appetite" (OMB Circular A-123, p. 10).

Identify the relationship between risks and controls in the federal government environment. Because of the influence and history of the GAO and its emphasis on ensuring public funds are spent responsibly, internal controls and audit are important in the federal government. In its mission to improve the performance, integrity, and reliability of the federal government the incorporation of internal controls into almost all agency management processes is a prerequisite for effective risk management. Controls are techniques and mechanisms that provide assurance that entity objectives will be met. Objectives are organized into three general categories: operations, reporting and compliance. Finally, controls can be general (e.g., entity-level controls) or specific (e.g., transaction control activities) and are typically detailed in agency policy or procedures.

Traditionally, risk has been based on operational-specific execution and decisions regarding the trade-off between risk and opportunity based on project components such as cost, schedule and performance (Playbook: Enterprise Risk Management for the U.S. Federal Government, July 2016, p. 12). The control environment that evolved to address this traditional approach to risk was based on addressing risk reduction through application of discrete controls. Enterprise risk management (ERM) in the context of the federal government incorporates the legacy and foundation of internal controls coupled with traditional risks and incorporates them into a broader approach to managing risk at the enterprise level. The focus of ERM is on a portfolio view of both risk and opportunity that is based on strategy and mission, in addition to project specific considerations. The relationships among internal controls, risk management, enterprise risk management and governance as described are depicted in Figure 2-FED (OMB Circular A-123, p. 8).

Figure 2-FED
Relationship between ERM and Internal Controls and Enterprise Risk Management



Analyze federal government risk controls and other risk management initiatives according to federal government standards. Another defining characteristic of risk management in the federal government environment is the role and influence of various standards. A standard is an established norm or requirement, usually a formal document that establishes criteria, methods, processes and practices under the jurisdiction of an international, regional or national standards body. Whereas an ERM framework such as ISO 31000:2018 relates to a broad-based standard for implementing ERM, there are various other standards and frameworks relevant to the federal government environment. The NIST Enterprise Risk Management Framework is one such example. Furthermore, standards and frameworks in the federal government context frequently have corollaries in policy and or statute. In the case of the NIST Enterprise Risk Management Framework, policy comes from OMB Circular A-123 and one of the relevant statutes is the E-Government Act.

A federal government risk professional who has a clear understanding of the connections among and between statute, policy, framework and standards within the context of an agency's risk profile and strategic objectives is positioned to design better ERM approaches based on accurate analysis of the agency's business model, context, scope and governance.

Identify federal government reporting requirements. ERM reporting requirements are unique in the federal government context. All agencies, regardless of funding, focus and business model are subject to certain mandatory reporting requirements related to risk management. Additionally, some voluntary reports are also recommended to agencies to inform stakeholders about the effectiveness of ERM programs. Table 2-FED identifies reporting requirements based on source (i.e., internal or external) and whether or not they are mandatory or voluntary. Each report is classified as internal based on the potential for classified material to restrict or limit information sharing externally.

Table 2-FED
Reporting Requirements

Report / Source	Internal	External	Voluntary	Mandatory
Annual Assurance Statement	X[1]	X		X
Integration of ERM and Internal Control	X	X	X	
OMB Circular A-123, APX A	X	X	X	X
OMB Circular A-130, APX I[2]	X	X		X
FMFIA (AFRs and PARs)	X	X		X
Govt. Corp. management report	X	X		X

Understanding reporting requirements will not only ensure program compliance but, more importantly, help a risk professional develop an objectives-based approach to ERM that supports agency mission.

Distinguish between federal government requirements. Finally, OMB's Circular A-123 identifies five requirements for ERM in the federal government:

- Management is responsible for the establishment of a governance structure to effectively implement, direct and oversee implementation of the Circular and all the provisions of a robust process of risk management and internal control.
- Agencies must maintain a risk profile to provide a thoughtful analysis of the risks an agency faces toward achieving its strategic objectives arising from its activities and operations, and to identify appropriate options for addressing significant risks.
- After initial implementation, the agency's risk profile must be discussed each year with OMB as a component of the summary of findings from the agency strategic review and FedSTAT (See OMB Circular No. A-11, sec 270).
- Management must evaluate the effectiveness of internal controls annually using GAO's Standards for Internal Control in the Federal Government known as "The Green Book" (OMB Circular A-123, p. 1 and 2). As applicable, ERM must be integrated with management's evaluation of internal control. In addition, it is important for the risk professional to keep in mind that the assurance statement is for internal controls, not the risks themselves, and is not an assurance statement over the ERM implementation as a whole.
- The agency risk profile must be updated at least annually.

Additionally, OMB's Circular A-123 makes additional recommendations for effective implementation of ERM in the federal government by suggesting that:

- Implementation of the Circular should leverage existing offices or functions within the organization that currently monitor risks and the effectiveness of the organization's internal control, and
- Agencies should develop a maturity model approach to the adoption of an ERM framework. For FY 2016, agencies were encouraged to develop an approach to implement ERM. For FY 2017 and thereafter agencies must continuously build risk identification capabilities into the framework to identify new or emerging risks and/or changes in existing risks.

Effective risk management professionals in the federal government will have a clear understanding of OMB's requirements and "presumptively mandatory requirements" (OMB Circular A-123, p. 2) regarding implementation of the Circular and be able to meet them in a timely fashion.

Self-Assessment of Content Areas. Table 3-FED is the self-assessment for the domain area of "Understanding the Federal Government Risk Management Environment." Please fill it out based on your self-ranked proficiency in each of the duties. Self-score your knowledge and understanding of each task based on a 5-point scale with 1 being the weakest and 5 being the strongest. Then, sum the scores and divide by the total number of tasks. Then, enter the quotient into the box for "Domain." The activity will help you prioritize time for additional reading and studying. Enter only one score for each of the task areas. Remember, appendix B has a clean copy of the self-assessment worksheet that can be used multiple times to track your progress and shows all domains and tasks in one location.

Table 3-FED
Self-Assessment for the Domain Area of Understanding the Federal Government Risk Management Environment

Domain	Duties and Tasks	Self-Rank Score: Domain	Self-Rank Score: Task
A	**Understanding the Federal Government Risk Management Environment**		
	A.1 Identify sources of government information and reporting (e.g., GAO, OIG, Grantees)	divide by 6	
	A.2 Assess key stakeholders		
	A.3 Identify the relationship between risks and controls in the Federal government environment		
	A.4 Analyze Federal government risk controls and other risk management initiatives according to Federal government standards		
	A.5 Identify Federal government reporting requirements		
	A.6 Distinguish between Federal government requirements		
		Sum	

Sample Exam Question

According to federal guidance, what types of models are suggested to assist with the adoption of enterprise risk management?

A. Capability maturity models

B. Failure Modes and Effects Analysis (FMEA) models

C. Monte Carlo simulation models

D. Stochastic optimization models

Answer: A

Reference: OMB (July 15, 2016). Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control. Washington, DC: U.S. Government Printing Office. p. 2, 3rd bullet.

https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf

Domain 2: Risk Management Implementation in the Federal Government

The second competency domain in the RIMS-CRMP-FED micro-credential curriculum addresses certain unique considerations in the federal government environment that relate to implementing ERM in the federal government.

Learning Objectives

To successfully complete this portion of the examination, the certification candidate should be able to:

1. Communicate roles and responsibilities within the federal government ERM process.
2. Coordinate and work with stakeholders and partners (e.g., oversight bodies, internal, external, public or private sector, federal, state, local, tribal, territorial).
3. Engage federal government risk networks.
4. Develop two-way internal communication strategies on the federal government ERM process.
5. Align internal controls to balance risk and opportunities with federal government risk tolerance.
6. Implement risk controls and other risk management initiatives according to federal government standards (e.g., OMB, GAO, DOD, NARA, NIST).

Examples

Communicate roles and responsibilities within the federal government ERM process. Roles and responsibilities for ERM implementation begin with the risk professionals who need to maintain a cohesive approach to interaction with risk owners and others involved in the overall governance of the ERM implementation.

OMB's guidance from Circular A-123 regarding the role of a risk management professional emphasizes:

- Helping senior management develop and implement core policies.
- Ensuring risk levels and processes are consistent with risk tolerance.
- Supporting implementation of effective controls.
- Developing strong reporting and analysis systems.
- Identifying emerging risk, concentrations of risk and interdependencies among risks.
- Elevating critical issues to appropriate levels within an agency in a timely fashion.

A successful risk professional in the federal government context understands the importance of finding the appropriate risk owners who are responsible for the effective management of risks and opportunities in their agency. Moreover, the risk professional should provide tools and techniques that help inform decisions risk owners make regarding how to minimize downside and maximize upside within the agency while balancing relevant risks and rewards.

From a governance standpoint, it is equally important to communicate the difference between the roles of risk professionals versus those of risk owners in both documentation of process and other reporting such as risk dashboards and external reports. By maintaining a clear understanding of the governance structure, execution will be more efficient and the risk professional will be able to keep the buy-in and commitment needed to sustain the implementation through its continuous life cycle.

Coordinate and work with stakeholders and partners. One of the practical implications of assessing stakeholders (item two from the first competency domain) is the identification of interdependencies among and between risks, and the resources required to successfully execute programs and initiatives. Use of an approach to coordination based on the individuals who are responsible, accountable, need to be informed or need to be consulted (RACI) helps maintain clearer understandings regarding execution of either risk management or project management. The risk management professional can further support the process by identifying the risk tolerances of different stakeholders and partners and combining them into a common risk philosophy that has important implications for selection of risk treatments and the amount of risk that an agency may take in order to achieve objectives.

Engage federal government risk networks. At a tactical level, risk professionals work with the risk networks—comprising the stakeholders and partners identified above—in order to apply risk treatments in an effective fashion and develop organizational risk competency.

Following through on effectiveness of risk treatments is more productive when a RACI methodology is utilized. Moreover, the risk professional can target training and coaching to support risk owners on the use of tools and methods such as risk registers, monitoring and reviewing, and measuring deviations from expected outcomes. Finally, effective communication is supported as well.

Develop two-way internal communication strategies on the federal government ERM process. Without clear and effective communication in all directions, the best designed approaches to ERM will not succeed. As a starting point, establishing a common language for the ERM implementation is helpful. For example, glossaries that clarify tools, techniques and the vocabulary of ERM avoid confusing situations where terms or acronyms may be the same but have different meanings within the agency. It can be as simple as understanding the
difference between a general ledger and general liability insurance.

Benefits of a clear communication process include:

- Effective meetings with risk owners, following through on risk treatments and support of goal achievement.
- Maintaining a clear distinction between risk ownership and process ownership.
- Establishment of a portfolio view on risk process (i.e., aggregation of risk measurements throughout the agency).
- Use of joint decision-making when applicable.
- Effective upward communication through dashboards and other reports that support governance roles in the process.

Align internal controls to balance risk and opportunities with federal government risk tolerance. Item three from the first domain above—Identification of the relationship between risks and controls in the federal government environment—laid the foundation for applying an integrated approach to risk management. The primary purpose of an enterprise-wide based approach to risk management is to move from the traditional position of reactive responses and transactional process to proactive risk treatments and interaction with risk owners to support the goals and objectives of the agency. Strong internal controls are an important component of an ERM implementation.

By leveraging traditional risk management tools and techniques, an effective risk management professional in the federal government supports:

- A forward-looking view of risk to drive strategy and business decisions.
- Identification of more risk management options through enterprise-level trade-offs.
- Explicit definitions of risk appetite and tolerance in order to allocate resources and make decisions about risk treatments.

Implement risk controls and other risk management initiatives according to federal government standards. This competency is the practical extension of item four from the first domain above—analysis of federal government risk controls and other risk management initiatives
according to federal government standards. After having identified the relevant interdependencies among frameworks and standards, policy and statutory requirements, the effective risk management professional works with risk owners to implement risk treatments and controls according to the applicable standard.

For example, at the beginning of its ERM implementation, an agency may develop a priority goal based on applicable statute and ensure that the required resources are applied to the goal in order to support compliance with the law. Conversely, as a result of applying gap analysis in the monitoring and reviewing stage of the risk process, an agency may identify new or revised standards that drive the development and incorporation of additional agency priority goals (APGs) based on the changing regulatory and enforcement environment that is unique to the federal government.

The federal government risk professional who has the ability to actively monitor the dynamic environment of standards will be more successful in delivering value to stakeholders.

Table 4-FED
Self-Assessment for the Domain Area of Designing Organizational Risk Strategies

Domain	Duties and Tasks	Self-Rank Score: Domain	Self-Rank Score: Task
B	**Risk Management Implementation in the Federal Government**		
	B.1 Communicate role and responsibilities within the Federal government ERM process		
	B.2 Coordinate and work with stakeholders and partners (e.g., oversight bodies, internal, external, public or private sector, Federal, State, Local, Tribal, Territorial)		
	B.3 Engage Federal Government risk networks		
	B.4 Develop two-way internal communication strategies on the Federal government ERM process		
	B.5 Align internal controls to balance risk and opportunities with Federal government risk tolerance		
	B.6 Implement risk controls and other risk management initiatives according to Federal government standards (e.g., OMB, GAO, DOD, NARA, NIST)		
		divide by 6	
		Sum	

Sample Exam Question

Which of the following establishes the requirement for agencies to develop, document and implement an information security and
protection program?

A. Federal Information Security Modernization Act

B. Information Security Forum

C. Information Technology Association of America

D. International Committee for Information Technology Standards

Answer: A

Reference: Federal Information Security Modernization Act of 2014, 44 U.S.C. §§ 113-283 (2014).

Domain 3: Risk Management Reporting in the Federal Government

The third competency domain in the RIMS-CRMP-FED micro-credential curriculum addresses some of the unique reporting requirements of the federal government environment.

Learning Objectives

To successfully complete this portion of the examination, the certification candidate should be able to:

1. Prepare internal reports according to Federal government reporting requirements.
2. Prepare external reports according to Federal government reporting requirements.
3. Report on the effectiveness of Federal government risk control according to standards (e.g., OMB, GAO, DOD, NARA, NIST).
4. Provide advice to federal officials on risk reporting and responses.

Examples

Prepare internal reports according to federal government reporting requirements. OMB's Circular A-123 identifies three deliverables related to an ERM implementation. The first is a report that describes the agency's ERM implementation approach and addresses governance
process—with an emphasis on risk philosophy, methodology for developing risk profiles and an implementation timeline. The second report is the risk profile of the agency and should be integrated with both the strategic plan of the agency and the president's budget. Finally, when internal controls have been identified as a component of the risk profile, a description of how ERM supports internal control must be incorporated into Agency Financial Reports (AFRs) or Performance and Accountability Reports (PARs) as applicable.

Prepare external reports according to federal government reporting requirements. This competency is the practical extension of item five from the first domain: identification of federal government reporting requirements. After the risk management professional has determined which reports are applicable to his or her agency, the process of integrating ERM into the communication flow begins. Two common reports that should incorporate information related to ERM are annual assurance statements and the AFRs and PARs required by the Federal Managers' Financial Integrity Act (FMFIA). Annual assurance statements address integration of ERM with internal control as well as risk control activities that fall outside of the traditional internal control process. AFRs and PARs, depending on maturity of the ERM program, may include detail on ERM governance (e.g., Risk management Councils,); and risks that may not have associated internal
controls that are addressed in the summary of corrective action plans or findings of material weakness.

Report on the effectiveness of federal government risk control according to standards. OMB's guidance from Circular A-123, combined with the GAO Green Book, are the primary standards that drive reporting requirements regarding effectiveness of risk control in the federal government environment. There are 17 principles and five internal control components that are described in the Green Book that relate to reporting on effectiveness of risk controls. When the principles are organized based on internal control component (see Figure 3-FED on next page), they are easier to understand and apply to ongoing internal control and ERM process.

The reporting requirements around effectiveness of internal controls are an integral part of the Circular A-123 from OMB and comprises reports that:

- are based on assessments of internal control,
- are based on summaries of internal control deficiencies,
- conclude on internal control principle evaluation and component evaluation, and
- conclude on overall assessment of systems of internal control.

An effective risk professional in the federal government environment will leverage the foundation of internal control evaluation into an ERM-based approach that evaluates an overarching system of internal and risk controls that reduces risks associated with achieving objectives. Moreover, an enterprise-wide approach will help manage opportunities as well as risks and support resource allocation based on risk tolerance.

Figure 3-FED
Internal Control Principles Organized by Component

Control environment	Risk assessment	Control activities	Information & communication	Monitoring activities
1. Demonstrates commitment to integrity and ethical values	6. Defines objectives and risk tolerances	10. Designs control activities	13. Uses relevant, quality information	16. Performs ongoing monitoring activities
2. Exercises oversight responsibilities	7. Identifies, analyzes and responds to risk	11. Selects and develops general controls for the information system	14. Communicates internally	17. Evaluates issues and remediates deficiencies
3. Establishes structure, authority and responsibility	8. Assesses fraud risk	12. Deploys and implements control activities	15. Communicates externally	
4. Demonstrates commitment to competence	9. Identifies, analyzes and responds to change			
5. Enforces accountability				

Provide advice to federal officials on risk reporting and responses. Competent risk management professionals in the federal government environment maintain a strong focus on risk ownership in order to ensure successful outcomes in selection and application of risk treatments. To provide advice to federal officials and assist them in making risk-informed decisions, risk management professionals may be less directly involved (e.g., a spectator or coordinator) or more involved (e.g., facilitator or strategic advisor).

Regardless of approach, the goal is to support both strategy and operations. Strategic planning is improved through incorporation of risk data that impact Agency Priority Goals (APGs) into regularly scheduled reviews. Operations are improved through decision-making that is informed by incorporation of risk appetite and tolerance considerations that support resource allocation and decisions regarding the balance between risk and reward associated with risk treatments.

The three competencies of the RIMS-CRMP-FED micro-credential, when combined with those of the core certification, create a valuable and unique opportunity for risk management professionals in the federal government to support the diverse missions of all agencies within the federal government.

Self-Assessment of Content Areas.

Table 5-FED
Self-Assessment for the Domain Area of Risk Management Reporting in the Federal Government

Domain	Duties and Tasks	Self-Rank Score: Domain	Self-Rank Score: Task
C	Risk Management Reporting in the Federal Government		
	C.1 Prepare internal reports according to Federal government reporting requirements		
	C.2 Prepare external reports according to Federal government reporting requirements		
	C.3 Report on the effectiveness of Federal government risk control according to standards (e.g., OMB, GAO, DOD, NARA, NIST)		
	C.4 Provide advice to federal officials on risk reporting and responses		
		divide by 4	
		Sum	

Sample Exam Question

According to OMB Circular No. A-123, agencies must develop a risk profile on an annual basis coordinated with their:

A. Leadership

B. Budget

C. Strategic reviews

D. Disaster recovery plans

Answer: C

Reference: OMB (July 15, 2016). Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control. Washington, DC: U.S. Government Printing Office. p. 2, 3rd bullet.

https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf

Appendix A-FED

Self-Assessment Checklist

Domain	Duties and Tasks	Self-Rank Score[1] Domain	Task
A	**Understanding the Federal Government Risk Management Environment**		
	A.1 Identify sources of government information and reporting (e.g., GAO, OIG, Grantees)		
	A.2 Assess key stakeholders		
	A.3 Identify the relationship between risks and controls in the Federal government environment		
	A.4 Analyze Federal government risk controls and other risk management initiatives according to Federal government standards (e.g., OMB, GAO, DOD, NARA, NIST)		
	A.5 Identify Federal government reporting requirements		
	A.6 Distinguish between Federal government requirements		
B	**Risk Management Implementation in the Federal Government**		
	B.1 Communicate role and responsibilities within the Federal government ERM process		
	B.2 Coordinate and work with stakeholders and partners (e.g., oversight bodies, internal, external, public or private sector, Federal, State, Local, Tribal, Territorial)		
	B.3 Engage Federal Government risk networks		
	B.4 Develop two-way internal communication strategies on the Federal government ERM process		
	B.5 Align internal controls to balance risk and opportunities with Federal government risk tolerance		
	B.6 Implement risk controls and other risk management initiatives according to Federal government standards (e.g., OMB, GAO, DOD, NARA, NIST)		
C	**Risk Management Reporting in the Federal Government**		
	C.1 Prepare internal reports according to Federal government reporting requirements		
	C.2 Prepare external reports according to Federal government reporting requirements		
	C.3 Report on the effectiveness of Federal government risk control according to standards (e.g., OMB, GAO, DOD, NARA, NIST)		
	C.4 Provide advice to federal officials on risk reporting and responses		
	Total		

Notes

1 Score your knowledge of each domain and task based on a 5 point scale with 1 being the weakest and 5 being the strongest.

2 By calculating your average score, you can compare yourself to yourself at different points in time.

Glossary

For a listing of many common terms and acronyms related to enterprise risk management, please see appendix F from CFO and PIC. (July 29, 2016). Playbook: Enterprise Risk Management for Federal Government. Washington, DC: U.S. Government Printing Office.

Exam References

CFO and PIC. (July 29, 2016). Playbook: Enterprise Risk Management for Federal Government. Washington, DC: U.S. Government Printing Office. https://cfo.gov/wp-content/uploads/2016/07/FINAL-ERM-Playbook.pdf

Committee of Sponsoring Organizations of the Treadway Commission. (June 2017). Enterprise Risk Management: Integrating with Strategy and Performance.

Department of Justice. (July 11, 2016). Department of Justice Guide to the Freedom of Information Act. https://www.justice.gov/oip/doj-guide-freedom-information-act-0

Government Accountability Office (Dec. 2016). Enterprise Risk Management: Selecting Agencies' Experiences Illustrate Good Practices in Managing Risk. (GAO Publication No. 17-63). Washington, DC: U.S. Government Printing Office. https://www.gao.gov/assets/690/681342.pdf

Government Accountability Office (July 2015). A Framework for Managing Fraud Risks in Federal Programs. (GAO Publication No. 15-593SP). Washington, DC: U.S. Government Printing Office. https://www.gao.gov/assets/680/671664.pdf

GPRA Modernization Act of 2010, 31 U.S.C. §§ 111-352 (2011). Chapter 5, Title 3, section 306(7). https://www.gpo.gov/fdsys/pkg/PLAW-111publ352/pdf/PLAW-111publ352.pdf

HM Treasury. (October 2004). The Orange Book: Management of Risk—Principles and Concepts. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/220647/orange_book.pdf

Increase in micro-purchase threshold was passed in the National Defense Authorization Act (NDAA) of 2018, Section 806, which updated Section 1902(a)(1) of title 41 U.S. Code.

Louisot, J-P, Ketcham, C; Enterprise-Wide Risk Management: Developing and Implementing (1st Ed). The Institutes.

National Archives and Records Administration website for General Records Schedules. https://www.archives.gov/records-mgmt/grs.html

National Institute of Standards and Technology. (March 2011). Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

National Institute of Standards and Technology. (May 2017). Draft NISTIR 8170, The Cybersecurity Framework: Implementation guide for ederal agencies. https://csrc.nist.gov/csrc/media/publications/nistir/8170/draft/documents/nistir8170-draft.pdf

OMB (July 15, 2016). Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control. Washington, DC: U.S. Government Printing Office. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf

OMB. (July 2017). Circular No. A-11, Preparation, Submission, and Execution of the Budget. Section 270. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/assets/a11_current_year/a11_2017.pdf

Paper Reduction Act of 1995, 44 U.S.C. §§ 104-13 (1995). Chapter 35, Title 4, 3502(3)(A)(i). https://www.gpo.gov/fdsys/pkg/PLAW-104publ13/html/PLAW-104publ13.htm

Responsibilities of holders, 32 C.F.R. § 2001.41 (2017). https://www.gpo.gov/fdsys/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-sec2001-40.pdf

Who is responsible for records management?, 36 C.F.R. § 1220.10 (2017). https://www.gpo.gov/fdsys/pkg/CFR-2017-title36-vol3/pdf/CFR-2017-title36-vol3-sec1220-10.pdf

Disclaimer

This guide is intended to provide only a general overview of the topics related to the RIMS-CRMP-FED micro-credential exam. This is not a complete analysis. The information provided is for general use only and is not intended to provide specific advice or recommendations, legal or otherwise, for any individual or organization. The information provided in this document is not mandatory to study nor does it guarantee a passing score on the RIMS-CRMP-FED micro-credential exam.

Contributors

Joseph A. Milan, PhD, ARM
Principal, JA Milan and Associates, LLC

SME Reviewers

Cynthia J. Vitters
Managing Director, Deloitte Advisory
Deloitte & Touche LLP

RIMS, the risk management society®, empowers risk professionals to make the world safer, more secure, and more sustainable. Through networking, professional development, certification, advocacy, and research, RIMS and its 80 chapters serves more than 200,000 risk practitioners and business leaders from over 75 countries. Founded in 1950, the Society publishes the award-winning Risk Management Magazine and produces RISKWORLD®, the largest annual gathering of global risk professionals. RIMS embraces diversity, equity, and inclusion and welcomes all risk professionals to connect and learn.

Version 5.0: Published April 2025