Certification Candidates Examination Guide

Contents

Introduction 3
Knowledge Based Examination 3
Body of Knowledge 3
1. Domains 3
Domain 1: Communication and Consultation 4
Domain 2: Establish the Context 4
Domain 3: Risk Assessment 5
Domain 4: Risk Treatment 5
Domain 5: Monitoring & Review 6
Domain 6: Governance 7
2. Knowledge and Practice Statements 9
3. Certification Requirements 9
4. Preparing for the Examination 9
5. Certification Examination 10
5.1 Examination Duration 10
5.1.1 CPRA 10
5.1.2 CPRM 10
5.2 Examination Questions 10
6. Disclaimer 11
Examination Practice Questions 12

Introduction

This guide has been developed to assist candidates to gain an understanding of the requirements to successfully pass the RMIA certification examination. The certification exam has been developed to assist candidates obtain professional qualifications recognised in Australia and, in the future, globally.

Certification may result in a positive impact on your chosen career in risk management and other like disciplines.

Certified Practicing Risk Associate (CPRA) has been designed for risk and business professionals who have a reasonable exposure to working with risk management that includes hands-on experience (1 to 3 years) with risk identification, assessment and evaluation, risk treatment, risk monitoring and reporting.

Certified Practicing Risk Manager (CPRM) has been designed for risk and business professionals who have 5 plus years 'hands-on' risk management experience.

Knowledge Based Examination

The Certification Exams have been developed as an knowledge based exam to determine your understanding and interpretation of the relevant Risk Management Standards. The use of semantics is important in identifying an applicant's underlying knowledge level of risk management.

Certification candidates are required to score **70%** to pass the examination.

Body of Knowledge

The RMIA has developed a Body of Knowledge (BOK) for those risk professionals seeking certification. This BOK comprises risk domains with reference to ISO31000:2009 Risk Management Standard and accompanying Knowledge and Practice Statements. These Knowledge and Practice Statements are generally agreed as both essential and generally known.

1. Domains

The certification focuses on the following domains, with reference to ISO31000:2009 Risk Management Standard:

Domain 1: Communication and Consultation

Domain 2: Risk Context

Domain 3: Risk Identification, Analysis and Evaluate

Domain 4: Risk Treatment

Domain 5: Monitoring and Review

Domain 6: Governance *****

* Domain 6 is not addressed specifically by ISO31000:2009 Risk Management Standard.

Domain 1: Communication and Consultation

Communication and consultation is concerned with identifying relevant stakeholders, the level of accountability, understanding their risk perceptions and decision making during all stages of the risk management process. The communication and consultation process includes, but is not limited to:

- Understanding stakeholder interests, perceptions and involvement in the risk management process.
- Involvement of stakeholders in the establishment of context and identification of risks.
- Ability to access stakeholders' expertise in analysing risks, defining risk criteria and evaluating the results.
- Using the results to report risks to risk and control owners as well as other stakeholders.
- Communication of treatment plans and enhancing change management process.
- Development of an appropriate external and internal communication and consultation plan.

Domain 2: Establish the Context

Establishing the Context is essential to ensure an effective risk management process. Context setting for the risk management process needs to take into account the organisational context including legal and regulatory environment, its objectives, values, culture, governance, roles, responsibilities, structure, operations, standards, guidelines, models, processes, systems, functions, information flow, decision making process, projects, services, assets and specific practices employed. In establishing the organisational context the organisation:

a. Articulates its objectives.
b. Defines the external & internal parameters to be taken into account when managing risk.
c. Sets the scope and risk criteria within the defined risk policy and framework.

Establishing the Context for the risk process relates to establishing the specific scope boundaries for a particular risk assessment process and has the following components:

a. Defining the goals & objectives of the risk management activities.
b. Defining responsibilities for and within the risk management process.
c. Defining the scope (including depth & breadth) of the risk management activities to be carried out (including specific inclusions and exclusions).

d. Defining the activities, process, function, project, process or activity and other projects, processes or activities of the organisation.
e. Defining the risk assessment methodologies.
f. Defining the way performance and effectiveness is evaluated in the management of risk.
g. Identifying & specifying the decisions that have to be made.
h. Identifying, scoping or framing studies needed, their extent and objectives, and the resources required for such studies.

Domain 3: Risk Assessment

Risk Assessment - identification, analysis, and evaluation is concerned with determining the severity of risk faced by the organisation and providing recommendations to business leaders on how to effectively manage risk within tolerance levels, including but not limited to:

- The creation of a risk profile that reflects the contexts of strategic and work operations (refer Domain 2).
- Identifying sources of risk, areas of impacts, events (including changes in circumstances), their causes and the potential consequences that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives.
- Analyse the risk severity associated with each threat, including anticipated risk consequence and likelihood using both quantitative and qualitative analysis techniques.
- Performing risk evaluations based on the outcome of the risk analysis, to assist in decision-making, informing which risks need treatment and the priority for treatment implementation.

This process includes the creation of a comprehensive, prioritised inventory of relevant risks, which is documented in a Risk Register.

Domain 4: Risk Treatment

Risks are assessed using the relevant risk criteria, appetite and ranked in an order of priority to indicate which risks are within tolerance or otherwise. Risks that fall outside of tolerance may need treatment.

Risk treatment is a risk modification process. It involves selecting and implementing one or more treatment options. Once the risk treatment has been implemented, it becomes a control or it modifies existing control(s).

There are a number of risk treatment options:

- Avoid the risk.
- Take or increase the risk in order to pursue an opportunity.
- Remove the risk source.
- Change the likelihood and/or consequences.

- Share the risk with another party or parties.
- Retain the risk by informed decision.

Risk treatment options will be determined with consideration to the organisation's risk appetite. Treatments are not mutually exclusive or necessarily appropriate in all circumstances.

Risk Treatment selection requires a balance between the costs and efforts of implementation against the potential benefits. This is a risk versus reward proposition. The treatment of risk entails the application of one or more mitigation strategies until the residual risk is deemed tolerable.

Types of risk treatment may include:

- Selection of an alternative amongst a hierarchy of controls (safety).
- System and procedural – changing the way things are done.
- Human resource management – for example training.
- Equipment – modifications or a more advanced solution.
- Hedging, insurance or re-insurance.
- A commercial solution.

All risk treatments are documented in the Risk Register or similar document.

Domain 5: Monitoring & Review

Both monitoring and review are part of the risk management process and involve regular checking or surveillance. A planned, resourced, approved and documented "Monitoring and Review" process and/or program is a critical component of the risk management framework and risk process.

A clear understanding and application of "Monitoring" and Review" for risks is required. The ISO31000 standard defines monitoring and review as follows:

a. Monitoring:

   Continual checking, supervision, critically observing or determining the status in order to identify change from the performance level required or expected; and

b. Review:

   Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives.

The monitoring and review processes are to encompass all aspects of the risk management process for the purposes of:

- Ensuring that controls are effective and efficient in both design and operation.
- Obtaining further information to improve risk assessment.

- Analysing and learning lessons from events (including near-misses), changes, trends, successes and failures.
- Detecting changes in the external and internal context, including changes to risk criteria and the risk itself, which can require revision of risk treatments and priorities.
- Identifying emerging risks.
- Capturing progress against risk treatments.

Organisations are to establish an assurance process to satisfy the board and executive management that the risk framework and risk management processes are working to keep risks within tolerances and that controls are working effectively. The monitoring and review program provides mechanisms regarding how the assurance process works.

Domain 6: Governance

Risk management is central to sound corporate governance. Corporate governance in its wider sphere is already dealt with under standard management practices each organisation defines for itself.

Risk governance which is the focus of Domain 6 is a subset of corporate governance in relation to setting roles and accountabilities for managing risks, having transparency within the organisation that risk registers are disclosed and managed, and giving assurances that the appropriate controls are in place and performing as designed.

There is an intrinsic relationship between Governance and Risk Management that is explained from understanding the meaning of the terms:

a. Governance; and
b. Risk Management.

Governance refers to the actions, processes, traditions and institutions by which authority is exercised and decisions are taken and implemented.[1]

Risk management is the coordinated activities to direct and control an organisation with regard to risk (ISO Guide 73:2009, definition 2.1)

Risk governance applies the principles of good governance to the identification, assessment, management and communication of risks.[2]

Risk Governance "refers to the institutions, rule conventions, processes and mechanisms by which decisions about risks are taken and implemented.."[3]

The ASX Corporate Governance Council has released a publication in relation to governance entitled Corporate Governance Principles and Recommendations (Principles). Of particular interest to risk managers is Principle 7.

The purpose of Principle 7 is to ensure that material business risks are dealt with by the whole of management and reported using appropriate disclosure and communication. Many unlisted companies including government and not-for-profit entities use the ASX Corporate Governance Guidelines as a benchmark to meet even though they aren't obliged to.

1. International Risk Governance Council
2. International Risk Governance Council
3. Risk Governance – Wikipedia

Risk Management framework is a set of components that provides the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation (ISO 31000:2009 pages "v" and 2 of).

The risk management framework is an integral part of the governance of an organisation. The framework establishes and defines as a minimum the following:

a. Commitment
b. Organisational Context
c. Risk Policies
d. Risk Criteria and Appetite
e. Risk Ownership and Accountability
f. Risk Resourcing
g. Integration of Risk into Organisational Processes
h. Communication and Reporting of Risk
i. Risk Monitoring/Review/Assurance/Mitigation Processes

NOTE:

It is recommended that risk professionals are familiar with the following key documents that establish the foundation and principles for Governance and Risk Management Governance in Australia and internationally. Domain 6 content has been broadly based on these.

a. ASX "Corporate Governance Principles & Recommendations 3rd Edition";
b. ACNC "Governance For Good" Guide for Charity Board Members;
c. AICD (Aust. Institute of Company Directors) "Good Governance Guidance Performance and other Guidance documents on governance;
d. Commonwealth Legislation: " Public Governance Accountability Act 2013"
e. Australian Standards:
   i. AS8000 Good Governance Principles & Part 8000.1-8000.4;
   ii. AS8015 " Corporate Governance of Information & Communication Technology";
   iii. AS/NZS ISO 31000 "Risk Management Principles & Guidelines";
   iv. AS/NZS HB 436 "Risk Management Guidelines Companion to AS/NZS ISO 31000".

2. Knowledge and Practice Statements

For each domain there are Knowledge and Practice Statements.

Knowledge Statements provide guidance on the risk management knowledge that the risk professional required to possess to successfully pass the examination. For example, Domain 3 - Risk Assessment there are ten (10) knowledge statements.

An example of one is shown below:

KS3.2 Risk Techniques (ISO31010) and tools for risk identification, categorisation, analysis and evaluation.

Practice Statements provide guidance on the risk management practice knowledge that a CPRA is required to possess to successfully pass the examination. For example, Domain 3 - Risk Assessment there are fourteen (14) practice statements.

An example of one if shown below:

PS3.6 - Risk analysis from assessing consequences, likelihood and the risk rating, and the influencing factors that can affect these.

3. Certification Requirements

To achieve the certification, candidates are required to:

a. Pass the applicable examination.
b. Provide documentary evidence upon request by RMIA to support the candidate's attestation of tertiary education and years of cumulative work experience performing the tasks of a risk professional across the Body of Knowledge - Domains.
c. Adhere to the RMIA Code of Professional Ethics.
d. Agree to meet the requirements of the RMIA Continuing Education Policy.

4. Preparing for the Examination

The certification exam draws heavily from:

1. ISO 31000:2009, Risk Management – Principles and guidelines.
   This Standard provides principles, framework and a process for managing risk.
2. ISO Guide 73:2009, Risk Management – Vocabulary
   This standard complements ISO 31000 by providing a collection of terms and definitions relating to the management of risk.

Good preparation for the certification examinations can be achieved through a plan of study. It is recommended that this plan of study include a very good understanding of both ISO31000:2009 and ISO Guide 73:2009 supported by ISO31010:2009.

Further, it is recommended due consideration is given to additional reading of:

- HB436:2013 Risk Management Guidelines – Companion to AS/NZS ISO 31000:2009

- HB327:2010 Communicating and Consulting about Risk.

5. Certification Examination

The examination questions are intended to measure and test the candidate's practical knowledge and the application of general risk management concepts, ISO31000 standard and ISO73 guide. All questions are of equal value and designed with one ***best*** answer.

It should be noted that the examination questions have been written by experienced risk professionals. Each question on the exam has been subject to a peer review with consideration of:

- CPRA and CPRM Proficiency Statements
- ISO31000:2009 Standard
- ISO31010:2009 Standard
- ISO 73:2009 Guide
- Body of Knowledge: Domain, Knowledge and Practice Statements
- RMIA Examination Question Development Guidelines
- Targeted certification candidate risk management experience (CPRA – 1 to 3 years and CPRM 5 plus years)

Certification candidates are required to score **70%** to pass the examination.

5.1 Examination Duration

5.1.1 CPRA

The examination has a duration of 2 hours consisting of 100 questions (approx. 1 minute and 20 seconds per question), which is in keeping with industry standards**.**

5.1.2 CPRM

The examination has a duration of 3 hours consisting of 150 questions (approx. 1 minute and 20 seconds per question).

5.2 Examination Questions

Each question has four options (answer choices). The candidate is asked to choose the correct answer from the options. The examination questions currently consist of the following percentages per Domain. However, RMIA reserves the right to change these percentages at any time without notice.

Domain 1: Communication and Consultation (15%)

Domain 2: Risk Context (15%)

Domain 3: Risk Identification, Analysis and Evaluate (30%)

Domain 4: Risk Treatment (15%)

Domain 5: Monitoring and Review (15%)

Domain 6: Governance (10%)

6. Disclaimer

RMIA has designed this guide primarily as an educational resource to assist candidates prepare for the certification examination. RMIA makes no assertion that the use of this guide will ensure a successful outcome. The guide should not be considered inclusive of all information required to pass the examination.

Examination Practice Questions

To assist the certification Candidate, the following practice questions are provided as a guide to the type and style of questions in the Examination.

Question 1: Which of the following options are the **MOST** relevant to assist in defining the Context?

Options:

A. Setting the boundaries to view the threats that may impede organisational objectives.
B. Identify threats that relate to external factors that need to be effectively controlled.
C. Projects are set in context to measure cost overruns and delays in completing tasks by planned dates.
D. Context describes the circumstances in which risks occur.

Answer: A

Justification:

A. It makes it easier for everyday staff who may not initially be familiar with formal risk management concepts to feel comfortable to identify the Risks that exist according to the Contexts of their operational work.
B. This is a partial answer.
C. This is an incorrect way of defining context.
D. This is incorrect, it is from identifying sources and causes that explain the circumstances.

Question 2: Which of the following options are the **BEST** to assist an organisation to select an appropriate risk treatment?

Options:

A. Recommendation from internal audit.
B. Approval by the organisation's insurer.
C. An analysis of the control costs and benefits.
D. An analysis of the costs to implement.

Answer: C

Justification:

A. Recommendation by Internal Audit is of assistance, but it is management's decision with regard to costs and benefits vs risk.
B. Approval of the organisation's insurer would not be required.
C. An analysis of costs and benefits for controls helps the organisation understand if it mitigates the risk to an acceptable level.

D. Analysis of the costs to implement is only one part of the control costs, you also are required to consider the benefits.

Question 3: What is the definition of risk identification?

Options:

A. Capturing a list of risks in a register.
B. Discussing and outlining the descriptions of risks.
C. Detailed process of explaining risks to others.
D. Process of finding, recognising and describing risks.

Answer: D

Justification:

A. The output of the process may be the capturing and recording of the risks identified in a register, but this is not the definition of the process phase.
B. Discussing and outlining the description of risks may assist in risk identification, but this is not definition of the process phase.
C. The output of the process may allow the detailed process of explaining risks to others, but this is not the definition of the process phase.
D. Process of finding, recognising and describing risks. (Clause 2.15)

Question 4: Which of the following would we include as stakeholders in a business risk management process?

Options:

A. Stakeholders that are affected by a decision or activity.
B. Stakeholders who receive reports on the status of risks.
C. Risk owners, treatment owners and decision makers.
D. Risk owners, treatment owners and management.

Answer: A

Justification:

A. The definition from ISO31000:2009 (Clause 2.13)
B. This is too limiting regarding who is deemed to be a stakeholder
C. These are key stakeholders of the process, but would result in many key stakeholders not being included.
D. These are key stakeholders of the process, but would result in many key stakeholders not being included.

Question 5: Managing risks via a Risk Register is the most common method of recording risks and risk treatments. What is the **PRIMARY** advantage of using a risk register to record risk treatment options?

Options:

A. For compliance and auditing control status.
B. For monitoring and reporting of risk and control status.
C. For quantitative modelling of risk profile.
D. For assigning risk treatment and ownership.

Answer: B

Justification:

A. Risk registers do provide a vehicle to demonstrate evidence for audits and compliance purposes but this is not the primary advantage.
B. The primary advantage of using a risk register is to record risk treatment options including ownership of the risk and treatment and the target date for implementation. A risk register also aids tracking and reporting on the status of the implementation of the treatment.
C. Risk registers do allow risks and residual risk outcomes to be modelled quantitatively but this is not the primary advantage of using a risk register to record risk treatment options.
D. Risk registers do identify ownership, but this is not the primary advantage of using a risk register to record risk treatment options.

Question 6: Which of the following options are the **MOST** important benefit from an effective risk awareness program?

Options:

A. No change in the number of incidents being reported.
B. Emerging risks are identified and part of decision making.
C. A quantitative evaluation of staff completing risk training.
D. Increased interest by staff on risk issues.

Answer: B

Justification:

A. The risk awareness programs are not getting the message across if the number of incidents being reported remains the same.

B. Identification of emerging risks is the major benefit.
C. To judge effectiveness of staff awareness training, measureable testing is necessary to confirm staff awareness. However, comprehension of what needs to be done does not ensure that action is taken when necessary.
D. May or may not provide meaningful feedback, but do not provide metrics.

Question 7: What is the definition of a risk profile?

Options:

A. Description of any set of risks.
B. Aggregated level of outcomes.
C. Types of risk in a register.
D. Categories used to define risks.

Answer: A

Justification:

A. The definition from ISO31000:2009 (Clause 2.20).
B. Consequence is part of the description of the risk, but doesn't contain are the information.
C. Types of risks in the register assist in the description of the risk profile, but are not the whole description.
D. Categories used can assist with the description of risk profile, but is not always used.

Question 8: Risk treatment plans are designed to reduce risk to:

Options:

A. A level that the business is willing to tolerate.
B. The point at which the benefit exceeds the expense.
C. A level that is too small to be measurable.
D. A rate of return that equals the current cost of capital.

Answer: A

Justification:

A. Risk should be reduced to a level that an organisation is willing to tolerate.
B. The business may or may not choose to pursue risk mitigation to the point at which the benefit equals or exceeds the expense.
C. Reducing the risk to a level too small to measure is not practical and is often cost-prohibitive.
D. Tying risk to a specific rate of return ignores the qualitative aspects of risk that must be considered.

Question 9: The architecture of Risk Management consists of the following key interdependent core elements:

Options

A. Context, design, implementation and monitoring.
B. Context, assessment, treatment, communication and monitoring.
C. Principles, framework and process.
D. Principles, framework and standards.

Key: C

Justification:

A. These are the components of the Risk Framework not the risk management architecture.
B. These are the components of the Risk Process not the risk management architecture.
C. These are the three parts of the Risk Management Architecture
D. There are two components of the architecture, but standards are not a component.

Question 10: The Board Risk Committee is required to evaluate risk management's performance. Which of the following options are the **KEY** factors to be considered in the evaluation?

Options:

A. Stakeholder engagement, accuracy, and relevance of risk reports.
B. Accuracy, completeness, relevance and timeliness of risk reports.
C. Accuracy, aggregation of risks, relevance, and timeliness of risk reports.
D. Stakeholder engagement, accuracy, and relevance and currency of risk reports.

Key: D

Justification:

A. These are key factors, but without the information being current there may be "missing" critical risk information that have a potential impact upon the organisation.
B. These are key factors, but without stakeholder engagement then the quality of the risk information and commitment to implement risk treatment(s) may be questionable.
C. Aggregation of risk is important, but not as important as A.
D. Stakeholder engagement is the key factor with accuracy, relevance and currency of risk reports.