BODY OF KNOWLEDGE

DOMAIN 6

GOVERNANCE

Purpose

To document the knowledge and practices, which an applicant for certification with RMIA is required to know to successfully pass the certification examination. The Body of Knowledge is to be read in conjunction with the appropriate Competency Statement.

Knowledge and Practice Statements are indicated in the tables below. The application of the Knowledge and Practice Statements may vary between the certification levels i.e. CPRA and CPRM, and this is indicated in the tables.

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 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".

Knowledge Statements

A certified risk professional is required to have knowledge of the following at the operational, project, process, and business/enterprise* activity levels:

Knowledge No.	Description	CPRA	CPRM
KS6.1	Standards (ISO31000, ISO 73), principles frameworks and practices related to facilitating the establishment of an organisation's governance framework.	√	*√
KS6.2	Defining a risk appetite approach.		√

Knowledge No.	Description	CPRA	CPRM
KS6.3	Communicating and consulting with stakeholders on the value of establishing a risk governance framework.		√
KS6.4	Defining the risk governance, policies and processes under the governance framework		√
KS6.5	Defining the roles and accountabilities for managing risk, policies and processes under the risk governance framework.		√
KS6.6	Defining the application of the risk governance framework aligning to the organisation's risk appetite and criteria.		√
KS6.7	Techniques for developing and implementing a risk governance framework based on all levels of management and assurance.		√
KS6.8	Embedding the risk governance framework into the organisational structure.		√
KS6.9	Defining the risk resources and capability to support the organisation's risk governance framework.		√
KS6.10	Techniques for verifying and validating that the risk governance framework supports the organisation's core business activities, governance framework, internal/external relationships, key obligations and processes.	√	*√
KS6.11	Defining the Risk Management Plan and Strategies.		√

Practice Statements

A certified risk professional is required to perform the following at the operational, project, process, and business/enterprise* activity levels:

Practice No.	Description	CPRA	CPRM
PS6.1	Collate information on organisational objectives, strategies, initiatives, processes, obligations and standards and have these aligned to the risk governance framework to optimise business activities.	√	*√
PS6.2	Develop a risk appetite approach and obtain senior management and Board approval.		√
PS6.3	Determine the organisation's risk capacity for risk appetite allocation by risk types.		√
PS6.4	Develop risk appetite statements and obtain senior management and Board approval.		√
PS6.5	Facilitate the development of an integrated risk governance framework that reflects the organisation's business context (legislative, regulatory, and other key obligations), organisational structure and business strategies/goals.		√

Practice No.	Description	CPRA	CPRM
PS6.6	Develop, document and obtain senior management and Board approval for the risk governance framework.		√
PS6.7	Develop, document and obtain senior management and Board approval for the risk management policies and strategies.		√
PS6.8	Develop, document and obtain senior management and Board approval for the risk management reporting framework.		√
PS6.9	Develop and document the risk management processes and tools that support the risk governance framework in consultation with the key stakeholders for their approval.		√
PS6.10	Facilitate the embedding of the risk governance and risk framework into the organisational structure and processes		√
PS6.11	Assign risk ownership, responsibility and accountability for and within the risk governance framework.		√
PS6.12	Develop and facilitate appropriate education and awareness of the risk governance framework.	√	*√
PS6.13	Validate that the allocated risk resources and capabilities adequately support the organisation's risk governance framework.		√
PS6.14	Implement techniques to give assurances to the board and management that the risk governance framework and associated policies and strategies reflect how risks are managed within risk tolerances as well as the organisation's risk capacity.		√
PS6.15	Develop and gain approval for the Risk Management Plan and Strategies.		√

*** At the enterprise level it is performed by the CPRM.**