P67 – Fundamentals of risk management

Diploma in Insurance

October 2017 Examination Guide

SPECIAL NOTICE

Candidates entered for the April 2018 examination should study this Examination Guide carefully in order to prepare themselves for the examination.

Practise in answering the questions is highly desirable and should be considered a critical part of a properly planned programme of examination preparation.

P67 – Fundamentals of risk management

Contents

Important guidance for candidates 3
Examiner comments 7
Question paper 10
Test Specification 16
Model answers 17

Published February 2018

Telephone: **020 8989 8464**
Fax: **020 8530 3052**
Email: **customer.serv@cii.co.uk**

IMPORTANT GUIDANCE FOR CANDIDATES

Introduction

The purpose of this Examination Guide is to help you understand how examiners seek to assess the knowledge and skill of candidates. You can then use this understanding to help you demonstrate to the examiners that you meet the required levels of knowledge and skill to merit a pass in this unit.

Before the examination

Study the syllabus carefully

This is available online at www.cii.co.uk or from Customer Service. All the questions in the examination are based directly on the syllabus. *You will be tested on the syllabus alone*, so it is vital that you are familiar with it.

There are books specifically produced to support your studies that provide coverage of all the syllabus areas; however you should be prepared to read around the subject. This is important, particularly if you feel that further information is required to fully understand a topic or an alternative viewpoint is sought. The reading list which can be found with the syllabus provides valuable suggestions.

Read widely

It is vital that your knowledge is widened beyond the scope of one book. *It is quite unrealistic to expect that the study of a single study text will be sufficient to meet all your requirements.* While books specifically produced to support your studies will provide coverage of all the syllabus areas, you should be prepared to read around the subject. This is important, particularly if you feel that further information is required to fully understand a topic or an alternative viewpoint is sought. The reading list which can be found with the syllabus provides valuable suggestions.

Make full use of the Examination Guide

This Examination Guide contains a full examination paper and model answers. The model answers show the types of responses the examiners are looking for and which would achieve maximum marks. However, you should note that there are alternative answers to some question parts which would also gain high marks. For the sake of clarity and brevity not all of these alternative answers are shown.

This guide and previous Examination Guides can be treated as 'mock' examination papers. Attempting them under examination conditions as far as possible, and then comparing your answers to the model ones, should be seen as an essential part of your exam preparation. The examiner's comments on candidates' actual performance in each question provide further valuable guidance. You can purchase copies of the most recent Examination Guides online at www.cii.co.uk. CII members can download free copies of older Examination Guides online at www.cii.co.uk/knowledge.

Know the structure of the examination
Assessment is by means of a three hour paper.

Part 1 consists of 14 compulsory questions, worth a total of 140 marks.

Part 2 consists of 2 questions selected from 3, worth a total of 60 marks.

Each question part will clearly show the maximum marks which can be earned.

Read the current Diploma in Insurance Information for Candidates
Details of administrative arrangements and the regulations which form the basis of your examination entry are to be found in the current Diploma in Insurance Information for Candidates brochure, which is *essential reading* for all candidates. It is available online at www.cii.co.uk or from Customer Service.

In the examination

The following will help:

Spend your time in accordance with the allocation of marks

- The marks allocated to each question part are shown on the paper.
- If a question has just two marks allocated, there are likely to be only one or two points for which the examiner is looking, so a long answer is a waste of time.
- Conversely, if a question has 12 marks allocated, a couple of lines will not be an adequate answer.
- Do not spend excessive time on any one question; if the time allocation for that question has been used up, leave some space, go on to the next question and return to the incomplete question after you have completed the rest of the paper, if you have time.

Take great care to answer the question that has been set

- Many candidates leave the examination room confident that they have written a 'good' paper, only to be surprised when they receive a disappointing result. Often, the explanation for this lies in a failure to fully understand the question that has been asked before putting pen to paper.
- Highlighting key words and phrases is a technique many candidates find useful.
- The model answers provided in this Examination Guide would gain full marks. Alternative answers that cover the same points and therefore answer the question that has been asked would also gain full marks.

Tackling questions

Tackle the questions in whatever order feels most comfortable. Generally, it is better to leave any questions which you find challenging until you have attempted the questions you are confident about. Candidates' should avoid mixing question parts, (for example, 1(a)(i) and (ii) followed by 2(b)(ii) followed by 1(e)(i)) as this often leads to candidates unintentionally failing to fully complete the examination paper. This can make the difference between achieving a pass or a narrow fail.

It is vital to label all parts of your answer correctly as many questions have multiple parts to them (for example, question 1(a) may have parts (i), (ii) and (iii)). Failure to fully distinguish between the separate question parts may mean that full credit cannot be given. It is also important to note that a full answer must be given to each question part and candidates should not include notes such as 'refer to answer given in 1(b)(i)'.

Answer format

Unless the question requires you to produce an answer in a particular format, such as a letter or a report, you should use 'bullet points' or short paragraphs. The model answers indicate what is acceptable for the different types of question.

Where you are asked to perform a calculation it is important to show **all** the steps in your answer. The majority of the marks will be allocated for demonstrating the correct method of calculation.

Provided handwriting is legible, candidates will **not** lose marks if it is 'untidy'. Similarly, marks are not lost due to poor spelling or grammar.

Calculators

If you bring a calculator into the examination room, it must be a silent, battery or solar-powered, non-programmable calculator. The use of electronic equipment capable of being programmed to hold alphabetical or numerical data and/or formulae is prohibited. You may use a financial or scientific calculator, provided it meets these requirements. The majority of the marks will be allocated for demonstrating the correct method of calculation.

EXAMINER COMMENTS

Question 1
There were some strong answers to part (b) of this question although few candidates could provide all four factors on which risk management depends, with some only stating the identifying risks factor.

Question 2
Some good answers were provided by candidates mostly where the different types of risks were understood and examples of each provided. However, some candidates confused pure risks with particular risks or pure risks with speculative risks and did not provide enough of a definition or examples in some instances regarding market risks.

Question 3
This question was well answered by the majority of candidates with good marks achieved by many, particularly in part (a).

Question 4
Many candidates answered part (a) well as they understood the definitions of risk appetite and risk tolerance and correctly explained each term. However, in part (b), there were some varied answers with few candidates achieving the full four marks for reputation risks, financial risks, strategic risks and operational risks. Some candidate answered this part of the question with a list of the risk standards such as FIRM, PESTLE etc or 'monetary, timing, administration' and not risks categories.

Question 5
The majority UK candidates explained the concept of control self assessment (CSA) but did not gain marks in part (b) relating to benefits to an organisation that applies to CSA. Some candidates did not achieve high marks on this question and answered it with a list of the steps in the risk management process.

Question 6
Few candidates gained high marks on this question, particularly in part (a), as they could not accurately explain the purpose and evolution of the UK Corporate Governance Code. In part (b), some candidates confused the requirements of the Companies Act or the Director's requirements with the recommended practices listed in the UK Corporate Governance Code. Some candidates provided a mixed list of the recommended practices and the Companies Act/Director's requirements.

Question 7
This question was well answered as most candidates correctly explained risk aware culture in part (a) and described the five activities of the LILAC acronym in part (b). Some International candidates listed the activities in the wrong order i.e. Learning which is the second 'L' in LILAC with Leadership which is the first 'L' and others could not describe each activity although may have been able to name it.

Question 8

The majority of candidates gained high marks on this question as they knew about questionnaires and checklists as a risk identification technique and they identified five advantages and five disadvantages. However, some candidates did provide some incorrect answers or duplications expressed in a slightly different manner in part (b). Credit was given to candidates who provided other advantages not listed in the model answer that were valid.

Question 9

This question was mostly well answered but some candidates quoted some of the other influences rather than those in the Renn and Rohrmann's structured framework. Some candidates were able to describe each level but not the title of each.

Question 10

There were some good answers to this question as candidates understood risk maturity and could correctly explain its importance in part (a). Many candidates listed either the 4Ns or the five levels of maturity listed in part (b) so achieved good marks overall.

Question 11

This question was well answered by UK candidates who, apart from two candidates, achieved high marks by either describing the various headings found in a risk register and providing examples of two risks, or by drawing the risk register in a matrix form. However, many International candidates did not perform well on this question, as rather than listing a specific risk for an example, they provided a risk category such as reputation risk or financial risk. Some candidates mentioned examples of other types of risk matrices that were not risk registers.

Question 12

Not many candidates performed well on the question with only one candidate achieving full marks. Many candidates gained a couple of marks but some candidates found this a difficult question to answer, with many just describing the differences between the two Acts. The Consumer Insurance (Disclosure and Representations) Act 2012 applies to consumers and the Insurance Act 2015 to commercial/non-consumer policyholders.

Question 13

The majority of candidates gained high marks on this question. There were some duplications of responsibilities for some of the roles i.e. risk officer and risk manager or chief risk officer, so marks were awarded where the candidate differentiated the responsibility if similar in the different roles. Some candidates misunderstood the question and just listed activities that a risk management function would undertake in both parts (a) and (b), rather than specific roles being identified in part (a).

Question 14

Very few candidates could supply all four key findings of the Penrose enquiry, although most candidates did attempt the question but with mixed results or provided reasons why risk management systems might fail or blaming the regulators.

Question 15

This was the most popular and well answered of the Part II questions. Many candidates could explain, in some detail, the additional services that a multi-national insurance broker may provide other than traditional insurance broking and achieved good marks in most cases. Many candidates correctly explained the business continuity management (BCM) process in part (a) and the importance of having a BCM plan and its benefits. However, some went on to mention the new international standard for business continuity management published in May 2012 by International Organization for Standardization (ISO) but could not quote the numeration of the standard as ISO 22301.

Question 16

This question was well answered by the majority of candidates who attempted it. Credit was given for other areas of issues relating to technology and cyber risks to the organisation. Candidates were able to use their own knowledge and experience of technology and cyber risks with more recent developments and examples of some recent incidents such as malware and ransomware attacks.

Question 17

This was the least well answered of the Part II questions. Some candidates found it difficult to explain the main purpose of internal audit of risk management in part (a). They then found it difficult to gain marks as they could not identify all the roles of the audit function in part (b) and the areas of risk management responsibility which it does not get involved in. Part (c), was also not very well answered in most cases.

THE CHARTERED INSURANCE INSTITUTE

P67

Diploma in Insurance

Unit P67 – Fundamentals of risk management

October 2017 examination

Instructions

- Three hours are allowed for this paper.
- **Do not begin writing until the invigilator instructs you to.**
- **Read the instructions on page 3 carefully before answering any questions.**
- Provide the information requested on the answer book and form B.
- You are allowed to write on the inside pages of this question paper, but you must **NOT** write your name, candidate number, PIN or any other identification anywhere on this question paper.
- The answer book and this question paper must **both be handed in personally by you** to the invigilator before you leave the examination room. **Failure to comply with this regulation will result in your paper not being marked and you may be prevented from entering this examination in the future.**

Unit P67 – Fundamentals of risk management

Instructions to candidates

Read the instructions below before answering any questions

- **Three hours** are allowed for this paper which carries a total of 200 marks, as follows:

Part I	14 compulsory questions	140 marks
Part II	2 questions selected from 3	60 marks

- You should answer **all** questions in Part I and two out of the three questions in Part II.
- You are advised to spend no more than two hours on Part I.
- Read carefully all questions and information provided before starting to answer. Your answer will be marked strictly in accordance with the question set.
- The number of marks allocated to each question part is given next to the question and you should spend your time in accordance with that allocation.
- You may find it helpful in some places to make rough notes in the answer booklet. If you do this, you should cross through these notes before you hand in the booklet.
- It is important to show each step in any calculation, even if you have used a calculator.
- If you bring a calculator into the examination room, it must be a silent, battery or solar-powered non-programmable calculator. The use of electronic equipment capable of being programmed to hold alphabetic or numerical data and/or formulae is prohibited. You may use a financial or scientific calculator, provided it meets these requirements.
- Answer each question on a new page. If a question has more than one part, leave six lines blank after each part.

PART I

Answer ALL questions in Part I

Note form is acceptable where this conveys all the necessary information

1. **(a)** State **four** factors on which risk management depends. **(4)**

(b) Illustrate the steps in the risk management process. **(8)**

2. Explain briefly the following **three** types of risk and provide an example for **each**:

(a) Pure risk. **(3)**

(b) Speculative risk. **(3)**

(c) Market risk. **(3)**

3. **(a)** State **four** advantages of insurance as a risk transfer mechanism. **(4)**

(b) Describe briefly **four** disadvantages of insurance as a risk transfer mechanism. **(8)**

4. **(a)** Explain briefly risk appetite and risk tolerance. **(4)**

(b) List **four** risk categories that an organisation might use when determining its risk appetite. **(4)**

5. **(a)** Explain control self assessment (CSA). **(5)**

(b) Describe briefly **four** benefits to an organisation that applies CSA. **(8)**

6. **(a)** Explain the purpose and evolution of the UK Corporate Governance Code. **(5)**

(b) State **five** recommended practices listed in the UK Corporate Governance Code. **(5)**

7. **(a)** Explain risk aware culture as it relates to an organisation. **(5)**

(b) Describe briefly the **five** activities that promote a risk aware culture known as LILAC. **(10)**

8. **(a)** Identify **five** advantages of using questionnaires as a means of risk identification. **(5)**

(b) Identify **five** disadvantages of using questionnaires as a means of risk identification. **(5)**

9. Describe briefly the **four** levels of risk perception in Renn and Rohrmann's structured framework. **(8)**

10. **(a)** Explain briefly risk maturity and its importance to an organisation. **(4)**

(b) Identify **four** levels within a risk maturity model that could be applied to an organisation. **(4)**

11. Produce an extract from a risk register containing **two** examples of potential risks to an organisation. **(12)**

12. Explain briefly the **three** significant differences between the duty of fair presentation in the Insurance Act 2015, and the duty to take reasonable care not to make a misrepresentation under the Consumer Insurance (Disclosure and Representations) Act 2012. **(6)**

13. **(a)** Identify **three** roles within the risk management function of an organisation. **(3)**

(b) Describe briefly **two** responsibilities, for **each** role identified in **part (a)** above. **(6)**

14. Describe briefly the **four** key findings of the Penrose enquiry, relating to non-executive directors at the time of the Equitable Life collapse in 2000. **(8)**

PART II

Answer TWO of the following THREE questions
Each question is worth 30 marks

15. You are a risk management specialist working for a multi-national insurance broker. The new business team has asked you to join them in a presentation to a potential new client, who is concerned about their lack of business continuity arrangements.

(a) Explain the importance and benefits of a business continuity management programme and include an explanation of the standards relating to business continuity. **(15)**

(b) Explain the additional services that you can provide, other than traditional insurance broking, in supporting the potential new clients risk management arrangements. **(15)**

16. You are a risk manager of a large financial organisation. In view of recent cyber attacks on other organisations, the Board has asked you to report to them on technology and cyber risks.

(a) Explain, with justification, **three** significant threats of technology and cyber risks to the organisation. **(15)**

(b) Describe how the organisation could protect itself from the **three** significant threats identified in **part (a)** above. **(15)**

17. You are the Internal Audit Manager for a general insurance company. At a recent board meeting, you were asked to prepare for an internal audit of the risk management process.

(a) Explain the purpose of the internal audit process. **(5)**

(b) Describe the role and assurances provided by the Internal Audit Team in relation to risk management. **(20)**

(c) Explain the actions that the Internal Audit Team will undertake before they begin a risk management audit. **(5)**

TEST SPECIFICATION

October 2017 Examination – P67 Fundamentals of risk management	
Question	Syllabus learning outcome(s) being examined
1	3 – Understand the core elements of the risk management process
2	4 – Understand the different categories of risk
3	6 – Understand the position of insurance within risk management
4	3 – Understand the core elements of the risk management process 4 – Understand the different categories of risk
5	3 – Understand the core elements of the risk management process
6	3 – Understand the core elements of the risk management process
7	2 – Understand the role and purpose of risk management
8	3 – Understand the core elements of the risk management process
9	1 – Understand the meaning of risk
10	5 – Understand current trends in risk management
11	3 – Understand the core elements of the risk management process
12	6 – Understand the position of insurance within risk management
13	2 – Understand the role and purpose of risk management
14	7 – Understand the key risk management lessons learnt from major loss events
15	2 – Understand the role and purpose of risk management 3 – Understand the core elements of the risk management process 6 – Understand the position of insurance within risk management
16	2 – Understand the role and purpose of risk management 4 – Understand the different categories of risk
17	2 – Understand the role and purpose of risk management 3 – Understand the core elements of the risk management process 7 – Understand the key risk management lessons learnt from major loss events

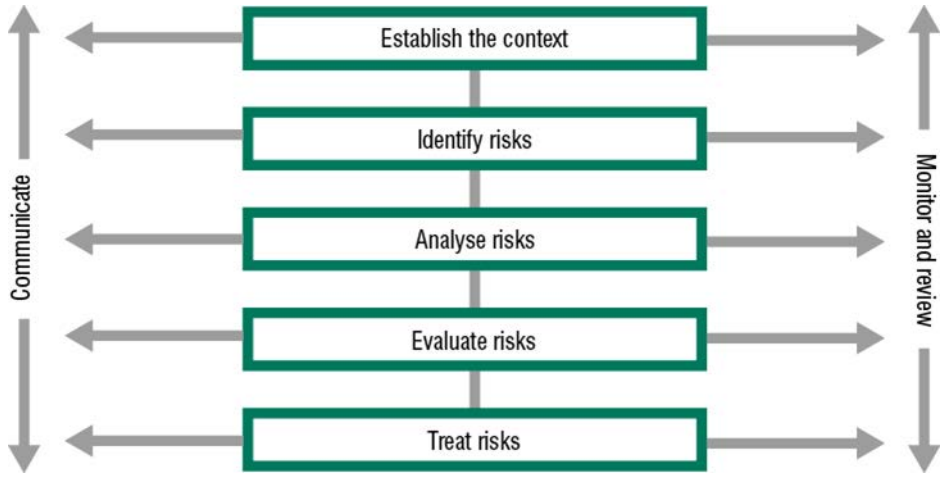
NOTE ON MODEL ANSWERS

The model answers given are those which would achieve maximum marks. However, there are alternative answers to some question parts which would also gain high marks. For the sake of clarity and brevity not all of these alternative answers are shown. An oblique (/) indicates an equally acceptable alternative answer.

Model answer for Question 1

(a)
- Identifying risks involved in an organisation.
- Estimating how often those risks are likely to materialise.
- Measuring potential consequences.
- Exploring options available to exercise some degree of risk control.

(b)



Model answer for Question 2

(a) Pure risk – a category of risk in which loss is the only possible outcome; there is no beneficial result. Pure risk is related to events that are beyond the risk taker's control and therefore a person cannot consciously take on pure risk. An example would be a house fire.

(b) Speculative risk – where someone deliberately chooses to place money or other resources at risk in the hope of obtaining a positive outcome. However, there is a downside risk if things do not turn out as expected/predicted. Examples would be gambling, investing in a new product.

(c) Market risk – also known as systematic risk is concerned with the risk of losses in trading positions arising from movement in market prices e.g. equity, interest rates, currency and commodity price movement and changes. Largely driven by economic factors, market risks can be heavily influenced by events such as natural disasters, recessions, political turmoil or terrorist attacks. Examples can include equity risk, property price risk and solvency risk.

Model answer for Question 3

(a) *Any four of the following:*

- Insurance is an economic vehicle for sharing exposures with a large number of organisations.
- Insurers have a wealth of experience in risk and risk funding mechanisms.
- Insurers can provide additional services which organisations find useful.
- Fast access to large insurance funds means an organisation has more cash for long-term investment as it has less need for liquid funds (in event of damage/loss).
- Premiums may be tax deductible.

(b) *Any four of the following:*

- Insurers are constrained by their need to measure all losses in monetary terms.
- In order for insurers to be able to assess and cost risks, they traditionally have cause of loss as their primary interest. The organisation sees impact, not cause, as the main concern. Insurers may not cover all possible causes of loss or damage.
- Insurers usually want to contain risk acceptance and pricing to a short period of time, often 12 months. An organisation needs to forecast for a longer period of time in its product design, product pricing and marketing strategies.
- Elements that make up an insurance premium (including potential claims costs, expenses of the insurer and insurer's profit) may not all be adding value to an insured organisation. Fund swapping or pound swapping.
- Insurers may demand detailed information in a format that suits them rather than the customer and risk control measures that an organisation may not consider cost effective.
- Organisations may have difficulty ensuring that insurer's conditions and warranties are met.
- Products offered by insurers are increasingly unlikely to include those risks that are of the greatest concern to a large organisation e.g. brand value, business and financial control, supply chain failure and intellectual assets.

Model answer for Question 4

(a) Risk appetite is the extent to which an organisation will tolerate risk. It is an organisation's attitude to risk and the risks that an organisation is actively willing to take.

Risk tolerance describes those risks that an organisation might be able to put up with.

(b)

- Reputation risks.
- Financial risks.
- Strategic risks.
- Operational risks.

Model answer for Question 5

(a) Control self assessment (CSA) is a process of self-review or self-audit applied systematically across an organisation at various levels. The approach and process are established beforehand, usually by risk management staff in conjunction with an audit.

CSA requires operational management and staff to self-review or self-audit risk controls for which they are responsible and to communicate the results up through the appropriate management line. The risk management department will follow up or request further clarification if needed. CSA is used in conjunction with a monitoring process and is subject to a periodic audit to check that it is delivering trusted and useful information.

(b) *Any four of the following:*

- Obtain a clear and shared understanding of major activities and objectives of business units and processes.
- Foster improved awareness of risk and controls among management and staff.
- Provide a flexible but structured approach to improving the organisation's controls framework.
- Enhance responsibility and accountability for risks and controls among management and staff.
- Highlight best practices and opportunities to improve business performance.
- Standardise and benchmark processes, where the same functions are performed in multiple locations.
- Help directors to meet their corporate governance responsibilities.
- Reduce the time and effort it takes for internal auditors to gather information on business units and provide quicker focus on areas requiring attention.
- A useful way of ensuring compliance with corporate standards including risk aspects of legislation and other compliance needs.

Model answer for Question 6

(a) The UK Corporate Governance Code provides a code of best practice for companies listed on the London Stock Exchange. It has been in existence for some years but was substantially strengthened in 2003 to implement the recommendations of a series of major public reports on corporate processes and behaviour (Cadbury 1992, Greenbury 1995, Hampel 1998, Turnbull 1999 and Higgs 2003). It was originally a 'voluntary code' but in the Financial Conduct Authority (FCA) Listing Rules, the UK financial regulator requires public listed companies in all industries to disclose in their annual report and accounts how they have complied with the Code or explain where they have not complied with its recommended practices.

(b)

- Separation of duties of the roles of chairperson and chief executive officer (CEO).
- CEO employment contracts to have a time limit.
- The minimum numbers of non-executive directors on the Board.
- Specify the company's risk appetite.
- Board subcommittees to be established (i.e. audit, remuneration, nomination).

Model answer for Question 7

(a) Every organisation has its own way of doing things. An organisation's culture is a collective description reflecting typical behaviour patterns of people who work there. The way people behave at work is strongly influenced by the customs and practices of their organisation. As customs and practices are developed, encouraged or discouraged by management, behaviours and attitudes can be altered.

A risk aware culture, in the context of risk management, is where organisations must decide how they want to deal with risk and how staff should deal with risk and set out to create and sustain a risk aware culture.

(b)
- Leadership – in terms of clarification of strategic and personal risk objectives.
- Involvement – of stakeholders at all stages of risk management.
- Learning – from events with effective training.
- Accountability – of individuals but with shared efforts to prevent reoccurrence.
- Communication – with free discussion of objectives, methods and results.

Model answer for Question 8

(a)
- Cheap and efficient way of collating large amounts of information.
- Simple and easy to use.
- Useful way of updating information for current use and for monitoring trends against previous surveys.
- Can be adapted to individual areas of risk interest.
- Useful for putting diverse sources of information into a common format.

(b) *Any five of the following:*
- Can be completed by someone who may not be skilled in the subject matter.
- Can be completed by someone who may not understand precisely the objectives and ultimate use of the answers.
- Can focus the user's attention simply on answering the questions themselves, without keeping the overall reason for the questions in mind; a 'form filling exercise' rather than an opportunity to take the 'wider perspective'.
- Can be at risk of being ambiguous to the reader.
- Can be at risk of being completed too quickly and without much thought by someone who considers their time is better spent elsewhere.
- Can be at risk of being completed by someone who may have their own reasons for suppressing risk information.

Model answer for Question 9

- First level – collective reasoning strategies that have evolved over the years, independent of the nature of a risk. Primary mechanisms of selecting, memorising and processing signals to form an opinion about the seriousness of risk.
- Second level – knowledge of risk or at least what we believe from available information to be true. Recognises that emotional factors are important. Whether the consequence of a risk is seen as good or bad will colour a person's attitude to the risk.
- Third level – social, political and economic culture concerns the social and political institutions that people associate with a risk or its cause. People's views are shaped by the views of their reference group.
- Fourth level – personal identity and views affect risk perception and govern many of the lower levels of influence. Perception of risk is shaped by the society in which we live.

Model answer for Question 10

(a) Generally speaking, organisations with effective risk management processes can expect less unexpected losses and better selection of future opportunities.

A qualitative indication of progress in developing risk awareness in an organisation can be obtained by regularly assessing the current level of risk culture. Processes of observation, audit and interviews are used to evaluate the extent to which risk culture is embedded in organisation procedures and practices. The result is a classification in terms of risk maturity. Various levels of maturity are defined by descriptions of risk control structures and perceived attitudes to management of risk.

(b) The 4Ns – four levels of maturity labelled:

- Naïve.
- Novice.
- Normalised.
- Natural.

Another example would be a model with five levels of maturity. These levels correspond to observable features of risk management behaviour as follows:

- Initial.
- Uncoordinated.
- Intermediate.
- Coordinated.
- Strategic.

Model answer for Question 11

Risk ID	Risk description or scope of risk	Likelihood	Impact (magnitude)	Overall rating (likelihood x impact)	Existing controls	Action to be taken	Risk owner
1.1	Loss of key manager		1	3	Medium		Organisational operational plans in place
1.2	Fire in factory		1	3	Medium		

Model answer for Question 12

- A commercial policyholder is still required to volunteer information.
- The duty of a commercial policyholder is to not misrepresent, rather than take reasonable care not to misrepresent.
- The Consumer Insurance (Disclosure and Representations) Act 2012 (CIDRA) rules are mandatory. An insurer may not use a contract term to put the consumer in a worse position than it would be under the provisions of CIDRA. By contrast, in non-consumer insurance, the parties may extend as well as reduce the duty of fair representation.

Model answer for Question 13

(a) *Any three of the following:*

- Chief risk officer.
- Risk manager.
- Risk officer.
- Member of a risk committee.

(b) *Any three of the following:*

Chief risk officer

- Ensure risk management at the heart of strategic decision making.
- Raise risk awareness across the organisation.

Risk manager

- Establish and oversee the approved risk management framework across a designated geographical or functional area of the business.
- Communicate on risk matters with designated business areas and external stakeholders.

Risk officer

- Help identify risk trends and emerging risks of interest to the organisation.
- Identify, analyse, assess and evaluate a range of individual risks in specified areas.

Member of a risk committee

- Assist in actively preparing and maintaining risk registers.
- Set detailed risk priorities.

Model answer for Question 14

The Penrose enquiry laid most blame on Equitable Life's senior executives and directors. Lord Penrose found that non-executive directors:

- did not understand risks to which Equitable Life was exposed to;
- were ill-equipped by training and experience to challenge actuaries;
- did not understand the financial position and;
- were influenced by the autocratic and domineering personality of Roy Ranson, joint actuary from 1982 and chief executive from 1992 to 1997.

Model answer for Question 15

(a) Organisations need to plan what they will do if a major incident occurs. This process is known as business continuity management (BCM). A plan is put into place to assist an organisation in understanding risks that could have an impact on their business e.g. a major fire at their warehouse/hotel, failure of utilities or a terrorist threat. The plan will also assist an organisation in anticipating incidents that could threaten its survival and to manage the consequences. The objective is to keep a system operational despite losses occurring and to restore it as quickly as possible to its original state. Plans and procedures put in place limit the extent of damage, financial or otherwise that a significant event may cause.

ISO 22301 is the new international standard for business continuity management published in May 2012 by the International Organization for Standardization (ISO). ISO 22301 covers the whole process of setting up and maintaining systems to deal with potential disruptions. The standard is split into ten main clauses and places a greater emphasis on monitoring performance and aligning BCM. It is a guide to both BCM planning processes and management of an overall programme through training, exercises and reviews to ensure that BCM plans stay current and up-to-date.

How a business continuity plan could benefit an organisation – understand risks that could have a significant impact on the business e.g. major fire, failure of utilities, terrorist threat, failure of IT systems or cyber attack. Be prepared and know how to respond to a significant risk incident that could affect the survival of the organisation, alternative premises, media statement, cascade communication to staff, facilities recovery and business continuity following the risk event etc.

(b) Aside from the traditional role of an insurance broker to: provide advice on selection of insurers; execute instructions and; provide, in the case of larger national or international firms, a risk survey service.

The role of the insurance broker has evolved to assist an organisation (their client) in achieving its risk management objectives.

The list of services is growing constantly with some brokers providing services 'in-house' through their own employees. Others may have arrangements with specialist companies or provide appropriate services with or alongside professional advisers. Legal and accounting services are typically organised this way.

As new risks emerge intermediaries or brokers will continue to develop targeted solutions e.g. new services dealing with cyber liability and computer crime; expertise in areas such as wind farm energy.

Some of the services provided by large international or national broker networks or intermediaries may include the following:

- Property surveys – the original risk consultancy service offered by brokers, usually provided as an 'in-house' service. These comprise of:
  - Underwriting surveys to determine the risk information needed by insurers to underwrite the risk i.e. construction of buildings, occupation, protections, sprinklers, housekeeping etc.
  - Risk control surveys to provide the broker's client with an expert assessment of risks inherent in the premises and their occupation with practical recommendations for controlling and eliminating those risks.
- Business continuity plans – can be provided as an extension of its property survey or as a dedicated service, encompassing a range of non-property matters. The aim is to assist the client to understand risks that could have an impact on their business e.g. a major fire at their central warehouse, failure of utilities or a terrorist threat. The broker will help the client to put a plan in place to deal with such eventualities so that the business can be back up and running in the shortest possible time.
- Business interruption reviews – these reviews examine a client's business model, such as stock production, use of subcontractors for manufacturing and assess dependence on customers and suppliers. Taking account of business continuity work or plans the client has in place, the aim is to assist in identifying risks to the business and quantifying the correct sum insured.
- Health and safety in the workplace reviews – with the growth of legislation following the Health and Safety at Work etc. Act 1974, some brokers extended their risk management offering to include workplace liability. However, the exponential growth of health and safety legislation and regulation has made it difficult for a broking firm to maintain the level of competency required in all possible occupations. It is likely that having identified a particular issue e.g. the need for noise assessments, the broker will contact a specialist provider for further reviews and recommendations.
- Liability surveys – a similar situation applies with liability surveys. A broker may identify a particular product risk and may subcontract further investigation to an expert, for example in food safety and product recall.
- Motor fleet risk management – where a broker is involved in motor fleet risk management it is likely that it will contract out most of the following services:
  - Review of driver handbooks and fleet management procedures.
  - 'Defensive driving' training – advanced skills training for fleet drivers, focusing on how to avoid accidents and safe driving.
  - 'At work' assessments.
  - The use of telemetrics (telematics) to monitor and improve driving skills.
- Environmental risk surveys – this is a highly specialised field and involves the assessing of environmental impact of the client's premises and occupation. This can include relevant current and historical exposures and is particularly important and useful in the acquisition and disposal of premises.
- Post-loss control services – some brokers go beyond processing a client's claim with insurers to providing active assistance in the event of a loss e.g. quantifying and submitting claims, providing guidance to stop any further damage and undertaking detailed negotiations with loss adjusters and insurers.

- Claims services can extend to include administration and handling of all claims with certain classes of insurance e.g. employers' liability or motor, especially if a significant proportion of any financial loss is retained by the organisation (client).
- Disaster recovery services – as an extension to post-loss control services, some brokers are involved in providing specific assistance in the event of a major loss e.g. a product recall incident, a major transportation accident or major fire. Services range from access to specialist public relations support to a full crisis management capability.

In addition, some larger international and global brokers offer services around captive management and self-insurance fund administration. Such brokers may also have resources to offer related services across the reinsurance market or provide guidance and management of a range of employee benefit provisions e.g. pensions and absentee management.

Model answer for Question 16

(a) Data concentration

Concentrating information in a central computer system with a common communications system servicing both internal and customer-facing staff is the most obvious risk. This risk creates a single point of failure, where previously information was widely dispersed. The more an organisation depends on this information, the more vital is its security against physical hazards to common equipment and electronic intrusion.

Recent marketing of 'the Cloud' underlines data concentration issues. It is advertised as a place to store programs and data instead of investing in and maintaining your own data storage or backup facility. It is simply a computer complex with vast amounts of data operated by third parties. Customers have no control over security arrangements and the legal aspects of data usage and ownership.

The data concentration can also lead to communication issues. For example: loss of communication with a call centre; media organisations reliance on satellite links to transmit international news and television programmes.

Human intervention

Computers are reliable and follow their programmed instructions faithfully. They are not subject to fatigue, error or distraction like human workers. When processing data fed in by humans or using human input to decide which programs to run, they are subject to human imperfection which will affect the results they produce.

Cyber crime

Computers become vulnerable when they are connected to other computers in the outside world. Once a two-way connection is established, malicious interference becomes possible as well as the communication for which the application was designed. Computers connected to the internet can be threatened by any malicious individual almost anywhere in the world, an opportunity for criminals that has been labelled cyber crime.

Cyber crime works by sending malicious program instructions over a network to interfere with (hack into) connected computers. Cyber crime is widespread and cannot be ignored e.g. most medium and large businesses will have suffered a malicious IT security incident during the past twelve months. Criminals can profit from access to commercially or politically sensitive information. Terrorists or others may simply want to prevent other computers from working or to cause them to send destructive commands. E.g. recent hacking of NHS Trust hospital computer systems in the UK and in several other countries – May 2017; Ransomware viruses.

(b) Data concentration

Organisations should ensure that systems are kept up-to-date with current developments. In addition, data systems should be backed up regularly and kept in a back-up system such as external hard drives ideally offsite in case of IT system failure/hacking. Use of systems such as 'the Cloud' should be carefully considered as customers/organisations have no control over security arrangements and legal aspects of data usage and ownership are not fully resolved.

Human intervention

Staff should be trained whenever new IT systems are introduced to ensure that mistakes are kept to a minimum. Also, where and when systems are used including protection of equipment such as laptops, tablets and smart phones and data by staff should be an important consideration. E. g. using WIFI systems in hotels, restaurants and coffee shops is not secure for accessing and sending sensitive data. Software must be protected from both careless and malicious human activity both at source, in design and testing procedures and in operation from misuse or cyber crime. Often computers will be programmed to deliberately restrict human input choices to improve output integrity. Another technique used is to record all human interventions to provide an audit trail or in some applications to allow programmes to rewind to a previous state to restore information.

Cyber crime

First line defences include installing security software from a reputable source and encrypting data streams. Additional design precautions, including duplication and perhaps private data networks, will be needed in critical applications where malfunctions could have serious repercussions. Staff training is again essential as malicious software is often sent as attachments to seemingly harmless messages or e-mails or often just malicious e-mails. Mail filter systems should be in place to prevent such e-mails reaching inboxes.

Model answer for Question 17

(a) According to the Institute of Internal Auditors (IIA), the aim of internal audit is to evaluate and contribute too improvement of governance, risk management and control process using a systematic and disciplined approach. Internal audit is expected by the Board of an organisation to provide assurance regarding several key functions, one of which is risk management. The main purpose of internal audit of risk management is to provide assurance to the Board that an effective enterprise risk management system is in place and operating effectively.

(b) The Internal Audit Team are looking to see if appropriate procedures are in place, if they are being followed, and if the risk management system is meeting the requirements of the Board. They consider if recommendations for improvement need to be made and prepare reports for the audit subcommittee and executive as well as carrying out follow-up reviews to check if recommendations have been implemented and improvements, if any, that were achieved.

An audit function monitors, comments and advises, but does not make risk management decisions and does not take responsibility for any risk management actions. Any extension of the audit role must therefore be confined to advisory work. Their skills can be harnessed as consultants, but they must avoid risk management activities.

Audit function will include:

- Assurance that key risks are adequately reported and managed.
- Assurance that risks are correctly evaluated.
- Assurance that risk management processes are effective.

The audit team need to consider if: significant risks are being identified and assessed; appropriate risk responses are selected in line with risk appetite decided by the Board and; relevant risk information is captured and communicated in a timely manner across the organisation and enables staff, management and the Board to carry out their responsibilities.

The audit team will concentrate only on those risks that affect achievement of stated objectives. It will check that risks responses (i.e. to reduce, transfer or retain risks in broad terms) correspond to agreed risk acceptance or tolerance levels and the overall risk profile of the organisation is as required. Effective communication of risk information is essential both in written and verbal exchanges and the audit team will be looking to see that both internal and external recipients are receiving, in good time, all the information they need.

Evaluation of risk exposure is important and so the Internal Audit Team will be looking to come to an informed opinion about reliability of information and effectiveness of management operations. Inevitably they will also have to consider whether or not the organisation has complied with relevant laws, regulations and contract wordings where this is appropriate.

(c) Before they can begin a risk management audit, the Internal Audit Team will have to familiarise themselves with the risk management framework, understand the terms of reference for the risk management function and be clear about its objectives. Members of the team have to thoroughly understand the objectives and processes of risk management. They will need to review access and fully appreciate the way any risk management systems, processes and procedures are carried out so that they can evaluate and test their effectiveness.