IT Training and
Professional Development

BCS Practitioner Certificate in Information Risk Management Syllabus

Version 4.2

December 2012

Contents

Change History

Version Number and Date	Changes Made
Version 4.2 December 2012	Removed the need for candidates to gain 65% across sections A and B but maintain the overall pass mark of 65% (65 marks).
Version 4.1 August 2012	ISEB replaced with BCS throughout document where appropriate. Changes to terminology to reflect standards – ISO Guide 73:2009 and ISO/IEC 27005:2011. Removal of reference to international information risk management standards (section 1.1.4) and property loss control (sections 3.2.5 and 4.1) and subsequent renumbering Addition of terms in section 2.4. Risk Retention added where appropriate. Update to pre-requisites. Additional time added to syllabus. Included a section to cover excerpts from BCS books
Version 4.0 March 2011	Added in Entry Criteria; Classroom Size, Trainer Qualification Criteria and Notice to Training Providers. Introduced Knowledge and Skills and Learning Levels. Changed learning hours from 34 to 36. Changed pass rate to 65% for Section A and B (was just Section 1). Included Information Assurance to Section 1. Included Risk Management and Controls to Section 2. Included Business Cases to Section 4.
Version 3.0 January 2011	Updated with minor amendments.
Version 2.0 January 2010	Reformatted with the BCS branding.

Introduction

This document is the syllabus for the BCS Practitioner Certificate in Information Risk Management, as administered by BCS, The Chartered Institute for IT.

This Certificate in Information Risk Management is intended for (but not limited to) those who are involved in the areas of information security and information assurance.
The module contains a number of practical sessions, designed to build on the 'taught' components of the module, and to encourage debate and the sharing of knowledge and experience between students.

The qualification promotes a hands-on approach to Information Risk Management, making use of current standards, enabling students to make immediate use of the module on their return to their organisations.

Objectives of the Information Risk Management Certification

On completion of this module, delegates will have a detailed understanding of:

- How the management of information risk will bring about significant business benefits
- How to explain and make full use of information risk management terminology
- How to conduct threat and vulnerability assessments, business impact analyses and risk assessments
- The principles of controls and risk treatment
- How to present the results in a format which will form the basis of a risk treatment plan
- The use of information classification schemes

The course includes a number of practical examples of Information Risk Management techniques.

Entry Criteria

There are no formal entry requirements but candidates will require an understanding of information assurance. It is recommended that candidates attend an accredited training course.

Format and Duration of the Examination

A three hour scenario based written examination consisting of:

Section A – multiple-choice questions
Answer all of the 10 questions – each answer carries 1 mark.

Section B – short answer questions
Answer all of the 6 questions – each answer carries 5 marks.

Section C – essay questions
Answer all 3 questions – each answer carries 20 marks.

Notice to Training Providers

Each major subject heading in the syllabus is assigned an allocated time. The purpose of this is to give both guidance on the relative proportion of time to be allocated to each section of an accredited course and an approximate minimum time for the teaching of each section. Training Providers may spend more time than is indicated and candidates may spend more time again in reading and research.

The total time specified in this syllabus is 36 hours of lecture and practical work.

The course may be delivered as a series of modules with gaps between them, as long as it meets all other constraints. Courses do not have to follow the same order as the syllabus.

The syllabus contains references to established standards. The use of referenced standards in the preparation of training material is mandatory. Each standard used must be the version quoted in the current version of this syllabus.

Additional Time for Candidates requiring Reasonable Adjustments due to a temporary or permanent disability

Candidates may request additional time if they require reasonable adjustments. Please refer to the reasonable adjustments policy for detailed information on how and when to apply.

Additional Time for Candidates whose business language is not English

An additional 45 minutes will be allowed for candidates sitting the examination

- in a language that is not their mother tongue, **and**
- where the language of the exam is **not** their primary business language,

Foreign language candidates who meet the above requirements are also entitled to the use of a paper dictionary (to be supplied by the candidate).

The candidate registration form asks for the candidate's business language, if this is not English then BCS will automatically allocate additional time.

Excerpts from BCS Books

Training Providers may include excerpts from BCS books in the course materials. If you wish to use excerpts from the books you will need a license from BCS to do this. If you are interested in taking out a licence to use BCS published material you should contact the Head of Publishing at BCS outlining the material you wish to copy and the use to which it will be put.

Syllabus Content

1 Concepts & Importance of information risk management (4 hours)

In this section, delegates will explore the overall concept of risk management and how it is used in business

1.1 The need for information risk management

1.1.1 Outline which parts of an organisation can make use of information risk management
1.1.2 Explain why information risk management is used and the regulatory framework that surrounds information risk management
1.1.3 Explain when information risk management should be used

1.2 The context of risk in the business

1.2.1 Explain why businesses must take account of risk
1.2.2 Describe the business benefits of information risk management
1.2.3 Explain the consequences of no information risk management

1.3 Review of information security fundamentals

1.3.1 Describe the concept of confidentiality
1.3.2 Describe the concept of integrity
1.3.3 Describe the concept of availability
1.3.4 Other concepts, including accountability, non-repudiation, authenticity, identification and reliability
1.3.5 Describe the concept of information assurance

1.4 The use of international information risk management standards

1.4.1 Explain the need for and the uses of international information risk management standards

2 The information risk management environment (6 hours)

This section of the module examines the information risk management environment and terminology in greater detail.

2.1 Developing an information risk management strategy

2.1.1 The Risk management process, including identification, analysis, treatment and monitoring of risks
2.1.2 Perform a high-level risk assessment
2.1.3 Establish the business risk appetite and criteria for risk acceptance
2.1.4 Verify the business information security requirements
2.1.5 Verify the industry or sector legal and regulatory requirements
2.1.6 Agree an information classification scheme for information systems
2.1.7 Understand the appropriate industry or sector information risk management standards including terminology as described ISO Guide 73:2009 and ISO/IEC 27005:2011
2.1.8 Agreeing methods of treating risk, including avoidance/termination, reduction/modification, transference/sharing, acceptance/tolerance/retention
2.1.9 Different ways in which controls may be used - preventative, directive, detective and corrective.

2.2 Information risk management, risk assessment and risk treatment

2.2.1 Explain the concept of information risk management and ownership
2.2.2 Explain the concept of risk assessment
2.2.3 Explain the concept of risk treatment

2.3 Assets

2.3.1 Describe various types and the value of tangible assets
2.3.2 Describe various types and the value of intangible assets

2.4 Information risk management terminology

2.4.1 Explain the meaning of threats and hazards
2.4.2 Explain the meaning of vulnerabilities and proximity
2.4.3 Explain the meaning of likelihood or probability
2.4.4 Explain the meaning of risk
2.4.5 Explain the meaning of controls
2.4.6 Explain the meaning of risk avoidance/termination
2.4.7 Explain the meaning of risk modification
2.4.8 Explain the meaning of risk transference/sharing
2.4.9 Explain the meaning of risk acceptance/tolerance/retention
2.4.10 Explain the meaning of risk appetite
2.4.11 Explain the meaning of risk aversion
2.4.12 Explain the meaning of risk aggregation
2.4.13 Explain the meaning of risk retention
2.4.14 Explain the meaning of residual risk

3 Stages of information risk management (12 hours)

This section of the module examines the process by which the earlier stages of risk management are carried out.

3.1 Setting the scope

3.1.1 Understand how to set the overall scope of an information risk management programme
3.1.2 Explain how to set the limits of the scope

3.2 Business Impact Analysis

3.2.1 Understand who should be involved in a Business Impact Analysis
3.2.2 Understand the appropriate approach for the type of organisation and for the type of event/incident
3.2.3 Explain the differences between qualitative and quantitative analyses
3.2.4 Understand generic Business Impact Analyses
3.2.5 Understand how to formulate a Business Interruption Cost in terms of Confidentiality, Integrity and Availability
3.2.6 Explain the uses of Cost of Failure analyses
3.2.7 Understand 'worst-case scenarios'
3.2.8 Carry out a Business Impact Analysis (practical work)

3.3 Threat and vulnerability assessment

3.3.1 Describe some of the most common threats and hazards
3.3.2 Explain how to establish potential threats
3.3.3 Explain how to identify potential vulnerabilities
3.3.4 Demonstrate an understanding of the motivation for threats and the responsibility for causing them
3.3.5 Describe how to set the criteria for assessing the likelihood or probability
3.3.6 Explain how to specify a suitable impact/likelihood scale
3.3.7 Understand the use of statistical or historic data to predict likelihood
3.3.8 Carry out a Threat and Vulnerability assessment (practical work)

3.4 Risk determination

3.4.1 Demonstrate the use of a risk matrix
3.4.2 Explain how to quantify the results of a risk assessment
3.4.3 Place the results of the previous exercises into a risk matrix; identify the key risks for treatment and those that will be accepted (practical work)

3.5 Information risk management controls

3.5.1 Recommend suitable controls to treat the key risks from the previous matrix (practical work)
3.5.2 Describe the uses and benefits of a root cause analysis
3.5.3 Explain the various types of controls such as people, physical, procedural and technical

4 Action and implementation (7 hours)

This section of the module examines the process by which the latter stages of information risk management are carried out

4.1 Risk reporting and presentation

4.1.1 Understand the requirements for reporting on an information risk management programme
4.1.2 Produce a management report showing overall status; main areas of risk; key business impacts; key threats and vulnerabilities; recommended remedial action (practical work)

4.2 Business cases

4.2.1 Explain the need for a business case
4.2.2 Describe business case preparation and format
4.2.3 Understand business case presentation

4.3 Decision making

4.3.1 Explain the process of risk acceptance/tolerance/retention
4.3.2 Explain the process of risk avoidance/termination
4.3.3 Explain the process of risk transference/sharing
4.3.4 Explain the process of risk reduction/modification
4.3.5 Explain the purpose of a risk register

4.4 Risk treatment

4.4.1 Understand the requirements for the management of a plan to treat the risks identified
4.4.2 Explain the concept of business continuity and disaster recovery as additional methods of treating risk
4.4.3 Produce a treatment plan showing the review of selected controls; agreement of actions; establishment of ownership, accountability and responsibility; setting of realistic time scales; gaining business approval (practical work)

4.5 Risk monitoring

4.5.1 Explain the need for periodic reviews
4.5.2 Describe a process for ongoing reporting of the information risk management status

5 Information classification schemes (4 hours)

This section of the module examines the means by which information is classified in order to assist with the development of a Business Impact Analysis and the handling of information.

5.1 Classification process

5.1.1 Establish the importance of information classification
5.1.2 Explain the process for identifying and documenting information assets
5.1.3 Understand the verification process through the interviewing of information owners
5.1.4 Describe the use if Confidentiality, Integrity and Availability in the development of an information classification scheme
5.1.5 Explain the requirements for a periodic review of information and its classifications

5.2 Classification issues

5.2.1 Discuss the requirements for setting information classification
5.2.2 Describe the considerations for appropriate information storage
5.2.3 Describe the considerations for appropriate information disposal, transfer, transmission and processing

5.3 Typical classification schemes

5.3.1 Describe the main differences between various classifications such as – Strictly Confidential; Confidential; Unclassified
5.3.2 Understand the differences between information classification and privacy marking and handling
5.3.3 Produce an information classification scheme for confidential and strictly confidential information showing recommended controls for the handling of sensitive information (practical work)

Additional Information

This course will provide candidates with the levels of knowledge highlighted within the following table, enabling them to develop the skills to operate at the levels of responsibility indicated. The levels of knowledge, skill and responsibility are explained in the following text:

Level	Levels of knowledge	Levels of skill and responsibility
7		Set strategy, inspire and mobilise
6	Evaluate	Initiate and influence
5	Synthesise	Ensure and advise
4	Analyse	Enable
3	Apply	Apply
2	Understand	Assist
1	Remember	Follow

Levels of Skill and Responsibility

The levels of knowledge above will enable candidates to develop the following levels of skill to be able to operate at the following levels of responsibility (as defined within the SFIA framework) within their workplace:

Level 1: Follow

Work under close supervision to perform routine activities in a structured environment. They will require assistance in resolving unexpected problems, but will be able to demonstrate an organised approach to work and learn new skills and apply newly acquired knowledge.

Level 2: Assist

Works under routine supervision and uses minor discretion in resolving problems or enquiries. Works without frequent reference to others and may have influence within their own domain. They are able to perform a range of varied work activities in a variety of structured environments and can identify and negotiate their own development opportunities. They can also monitor their own work within short time horizons and absorb technical information when it is presented systematically and apply it effectively.

Level 3: Apply

Works under general supervision and uses discretion in identifying and resolving complex problems and assignments. They usually require specific instructions with their work being reviewed at frequent milestones, but can determines when issues should be escalated to a higher level. Interacts with and influences department/project team members. In a predictable and structured environment they may supervise others. They can perform a broad range of work, sometimes complex and non-routine, in a variety of environments. They understand and use appropriate methods, tools and applications and can demonstrate an analytical and systematic approach to problem solving. They can take the initiative in identifying and negotiating appropriate development opportunities and demonstrate effective communication skills, sometimes planning, scheduling and monitoring their own work. They can absorb and apply technical information, works to required standards and understands and uses appropriate methods, tools and applications.

Level 4: Enable

Works under general direction within clear framework of accountability and can exercise substantial personal responsibility and autonomy. They can plan their own work to meet given objectives and processes and can influence their team and specialist peers internally. They can have some responsibility for the work of others and for the allocation of resources. They can make decisions which influence the success of projects and team objectives and perform a broad range of complex technical or professional work activities, in a variety of contexts. They are capable of selecting appropriately from applicable standards, methods, tools and applications and demonstrate an analytical and systematic approach to problem solving, communicating fluently orally and in writing, and can present complex technical information to both technical and non-technical audiences. They plan, schedule and monitor their work to meet time and quality targets and in accordance with relevant legislation and procedures, rapidly absorbing new technical information and applying it effectively. They have a good appreciation of the wider field of information systems, their use in relevant employment areas and how they relate to the business activities of the employer or client.

Level 5: Ensure and advise

Works under broad direction, being fully accountable for their own technical work and/or project/supervisory responsibilities, receiving assignments in the form of objectives. Their work is often self-initiated and they can establish their own milestones, team objectives, and delegate responsibilities. They have significant responsibility for the work of others and for the allocation of resources, making decisions which impact on the success of assigned projects i.e. results, deadlines and budget. They can also develop business relationships with customers, perform a challenging range and variety of complex technical or professional work activities and undertake work which requires the application of fundamental principles in a wide and often unpredictable range of contexts. They can advise on the available standards, methods, tools and applications relevant to own specialism and can make correct choices from alternatives. They can also analyse, diagnose, design, plan, execute and evaluate work to time, cost and quality targets, communicating effectively, formally and informally, with colleagues, subordinates and customers. They can demonstrate leadership, mentor more junior colleagues and take the initiative in keeping their skills up to date. Takes customer requirements into account and demonstrates creativity and innovation in applying solutions for the benefit of the customer.

Level 6: Initiate and influence

Have a defined authority and responsibility for a significant area of work, including technical, financial and quality aspects. They can establish organisational objectives and delegate responsibilities, being accountable for actions and decisions taken by themselves and their subordinates. They can influence policy formation within their own specialism to business objectives, influencing a significant part of their own organisation and customers/suppliers and the industry at senior management level. They make decisions which impact the work of employing organisations, achievement of organisational objectives and financial performance, developing high-level relationships with customers, suppliers and industry leaders. They can perform highly complex work activities covering technical, financial and quality aspects. They contribute to the formulation of IT strategy, creatively applying a wide range of technical and/or management principles. They absorb complex technical information and communicate effectively at all levels to both technical and non-technical audiences, assesses and evaluates risk and understands the implications of new technologies. They demonstrate clear leadership and the ability to influence and persuade others, with a broad understanding of all aspects of IT and deep understanding of their own specialism(s). They take the initiative in keeping both their own and subordinates' skills up to date and to maintain an awareness of developments in the IT industry.

Level 7: Set strategy, inspire and mobilise

Have the authority and responsibility for all aspects of a significant area of work, including policy formation and application. They are fully accountable for actions taken and decisions made, by both themselves and their subordinates. They make decisions critical to organisational success and influence developments within the IT industry at the highest levels, advancing the knowledge and/or exploitation of IT within one or more organisations. They develop long-term strategic relationships with customers and industry leaders, leading on the formulation and application of strategy. They apply the highest level of management and leadership skills, having a deep understanding of the IT industry and the implications of emerging technologies for the wider business environment. They have a full range of strategic management and leadership skills and can understand, explain and present complex technical ideas to both technical and non-technical audiences at all levels up to the highest in a persuasive and convincing manner. They have a broad and deep IT knowledge coupled with equivalent knowledge of the activities of those businesses and other

organisations that use and exploit IT. Communicates the potential impact of emerging technologies on organisations and individuals and analyses the risks of using or not using such technologies. They also assess the impact of legislation, and actively promote compliance.

Levels of Knowledge

The following levels of knowledge shall be defined and applied for syllabus creation. Each topic in the syllabus shall be examined according to the learning objectives defined in the section devoted to that topic. Each learning objective has a level of knowledge (K level) associated with it and this K level by association defines the nature of any examination questions related to that topic.

Note that each K level subsumes lower levels. For example, a K4 level topic is one for which a candidate must be able to analyse a situation and extract relevant information. A question on a K4 topic could be at any level up to and including K4. As an example, a scenario requiring a candidate to analyse a scenario and select the best risk identification method would be at K4, but questions could also be asked about this topic at K3 and a question at K3 for this topic might require a candidate to apply one of the risk identification methods to a situation.

Level 1: Remember (K1)
The candidate should be able to recognise, remember and recall a term or concept but not necessarily be able to use or explain. Typical questions would use: define, duplicate, list, memorise, recall, repeat, reproduce, state.

Level 2: Understand (K2)
The candidate should be able to explain a topic or classify information or make comparisons. The candidate should be able to explain ideas or concepts. Typical questions would use: classify, describe, discuss, explain, identify, locate, recognise, report, select, translate, paraphrase.

Level 3: Apply (K3)
The candidate should be able apply a topic in a practical setting. The candidate should be able to use the information in a new way. Typical questions would use: choose, demonstrate, employ, illustrate, interpret, operate, schedule, sketch, solve, use, write.

Level 4: Analyse (K4)
The candidate should be able to distinguish/separate information related to a concept or technique into its constituent parts for better understanding, and can distinguish between facts and inferences. Typical questions would use: appraise, compare, contrast, criticise, differentiate, discriminate, distinguish, examiner, question, test.

Level 5: Synthesise (K5)

The candidate should be able to justify a decision and can identify and build patterns in facts and information related to a concept or technique, they can create new meaning or structure from parts of a concept. Typical questions would use: appraise, argue, defend, judge, select, support, value, evaluate.

Level 6: Evaluate (K6)

The candidate should be able to provide a new point of view and can judge the value of information and decide on its applicability in a given situation. Typical questions would use: assemble, contract, create, design, develop, formulate, write.

Format of the Examination

This syllabus has an accompanying examination at which the candidate must achieve a pass score to gain the BCS Practitioner Certificate in Information Risk Management.

Type	Written Examination, 10 multiple choice questions, 6 short answer questions and 3 essay style questions (all compulsory).
Duration	3 hour examination. An additional 45 minutes will be allowed for candidates sitting the examination • in a language that is not their mother tongue, **and** • where the language of the exam is **not** their primary business language, Foreign language candidates who meet the above requirements are also entitled to the use of a paper dictionary (to be supplied by the candidate).
Pre-requisites	There are no formal requirements but candidates will require an understanding of information assurance. It is strongly recommended that candidates attend an accredited training course. BCS also recommends candidates achieve the Certificate in Information Management Principles (CISMP) prior to sitting the PCIRM exam.
Supervised / Invigilated	Yes
Closed Book	No reading materials allowed into the examination room
Pass Mark	65/100 (65%)
Distinction Mark	Not applicable
Delivery	Paper based examination only via an BCS Accredited Training Provider
Learning Hours	34 hours

Trainer Qualification Criteria

Criteria:	Trainers must hold the BCS Information Risk Management Certificate.

Classroom Size

Trainer to candidate ratio:	1:16 ratio