BCS Practitioner Certificate in Information Risk Management Syllabus

Version 6.2
March 2015
Contents

Change History ........................................................................................................................................2
Introduction .........................................................................................................................................3
Objectives ............................................................................................................................................3
Entry Criteria ........................................................................................................................................3
Format and Duration of the Examination .............................................................................................3
Duration and Format of the Course .........................................................................................................4
Additional time for candidates requiring Reasonable Adjustments due to a disability .................4
Additional time for candidates whose first language is not English ..................................................4
Excerpts from BCS Books ....................................................................................................................4
Syllabus ................................................................................................................................................5
1 The concepts and framework of information risk management (2 hours) ......................................5
  1.1 The need for information risk management .............................................................................5
  1.2 The context of risk in the organisation .....................................................................................5
2 Information risk management fundamentals (4 hours) ................................................................6
  2.1 Review of information security fundamentals .........................................................................6
  2.2 The use of information risk management standards and good practice guides .....................6
  2.3 The process of information risk management .........................................................................6
  2.4 Terms and definitions .............................................................................................................6
3 Establishing an information risk management programme (9 hours) ............................................7
  3.1 The information risk management programme requirements ...............................................7
  3.2 Development of the strategic approach to information risk management ..............................7
  3.3 Information classification .......................................................................................................7
4 Risk identification (9 hours) ............................................................................................................8
  4.1 Identification of assets ............................................................................................................8
  4.2 Business impact analysis .......................................................................................................8
  4.3 Threat and vulnerability assessment .......................................................................................8
5 Risk assessment (8 hours) ...............................................................................................................9
  5.1 Risk analysis ..........................................................................................................................9
  5.2 Risk evaluation .......................................................................................................................9
6 Risk treatment (2 hours) ..................................................................................................................9
  6.1 Risk treatment options, controls and processes .....................................................................9
  6.2 Risk treatment plans .............................................................................................................9
7 Presenting risks and business case (2 hours) ...............................................................................10
  7.1 Risk reporting and presentation ............................................................................................10
  7.2 Business case .......................................................................................................................10
8 Monitor and review (2 hours) .........................................................................................................10
  8.1 Information risk monitoring ...................................................................................................10
  8.2 Information risk review ........................................................................................................10
Classroom Size ......................................................................................................................................11
Recommended Reading List ..............................................................................................................12
## Change History

Any changes made to the syllabus shall be clearly documented with a change history log. This shall include the latest version number, date of the amendment and changes made. The purpose is to identify quickly what changes have been made.

<table>
<thead>
<tr>
<th>Version Number and Date</th>
<th>Changes Made</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 6.2 March 2015</td>
<td>Updated language requirements for extra time and use of dictionaries. Standardised the trainer requirements.</td>
</tr>
<tr>
<td>Version 6.1 July 2914</td>
<td>Changes to 2.4.2, 5.3, 6, and 7. Changes to candidates requiring extra time when sitting an exam which is not their first language.</td>
</tr>
<tr>
<td>Version 6.0 November 2013</td>
<td>Syllabus additions and changes to: 2.4.2, 2.4.3, 2.4.4, 2.4.5, 3.2.3, 3.3.1, 3.3.2, 3.3.6, 4.2.6, 4.3.1, 5.1.1, 5.1.3, 5.1.4, 7.1.2</td>
</tr>
<tr>
<td>Version 5.0 November 2013</td>
<td>Major update of syllabus, including references to newer standards.</td>
</tr>
<tr>
<td>Version 4.2 December 2012</td>
<td>Removed the need for candidates to gain 65% across sections A and B but maintain the overall pass mark of 65% (65 marks).</td>
</tr>
<tr>
<td>Version 4.1 August 2012</td>
<td>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.</td>
</tr>
<tr>
<td>Version 4.0 March 2011</td>
<td>Added in Entry Criteria; Classroom Size, Trainer Qualification Criteria and Notice to Training Organisations. Introduced Knowledge and Skills and Learning Levels. Changed learning hours from 34 to 36. Changed pass rate to 65% for Section A and included Information Assurance to Section 1. Included Risk Management and Controls to Section 2. Included Business Cases to Section 4.</td>
</tr>
<tr>
<td>Version 3.0 January 2011</td>
<td>Updated with minor amendments.</td>
</tr>
<tr>
<td>Version 2.0 January 2010</td>
<td>Reformatted with the BCS branding.</td>
</tr>
</tbody>
</table>
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 candidates.

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

Objectives

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.
Duration and Format of the Course

Candidates can study for this certificate in two ways: by attending training courses provided by Accredited Training Organisations or by self-study. An accredited training course will require a minimum of 36 hours of lecture and practical work run over a minimum of five days. The course can be delivered a number of different ways from traditional class-room based training to online e-learning.

Guidelines for Accredited Training Organisations

Each major subject heading in the syllabus is assigned a recommended 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 Organisations may spend more time than is indicated and candidates may spend more time again in reading and research.

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 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 first language is not English

If the examination is taken in a language that is not the candidate’s native / official language then they are entitled to 25% extra time.

If the examination is taken in a language that is not the candidate’s native / official language then they are entitled to use their own paper language dictionary (whose purpose is translation between the examination language and another national language) during the examination. Electronic versions of dictionaries will not be allowed into the examination room.

Excerpts from BCS Books

Training Organisations 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

1 The concepts and framework of information risk management (2 hours)

In this section of the syllabus, delegates will explore the overall concept of risk management and how it is used in the context of information risk.

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 it

1.1.3 Explain when information risk management should be used

1.2 The context of risk in the organisation

1.2.1 Explain why organisations must take account of risk

1.2.2 Describe the benefits of information risk management

1.2.3 Explain the consequences of not performing information risk management
2 Information risk management fundamentals (4 hours)

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

2.1 Review of information security fundamentals

2.1.1 Describe the concepts of confidentiality, integrity, availability

2.1.2 Describe the concepts of accountability, non-repudiation, authenticity, identification and reliability

2.1.3 Explain the difference between information security, information risk management and information assurance

2.2 The use of information risk management standards and good practice guides

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


2.2.3 Outline the information available from professional organisations such as the Institute of Risk Management

2.3 The process of information risk management

2.3.1 Explain the concept of information risk ownership

2.3.2 Describe the various stages of information risk management, including risk identification, risk analysis, risk evaluation and risk treatment

2.3.3 Explain the options for selecting risk management methodologies

2.4 Terms and definitions

2.4.1 Explain the meaning and interactions of threats, hazards, vulnerabilities, proximity, likelihood, probability and risk

2.4.2 Explain the meaning of strategic risk treatment, including risk avoidance or termination; risk reduction or modification; risk transference or sharing; risk acceptance or tolerance and risk retention

2.4.3 Explain the meaning of tactical risk controls, including preventative, detective, directive and corrective

2.4.4 Explain the meaning of operational risk controls, including physical or environmental, technical or logical and procedural or people
3 Establishing an information risk management programme (9 hours)

This section of the syllabus examines the requirements for an information risk management programme, the strategic nature of its approach and the need for information classification.

3.1 The information risk management programme requirements

3.1.1 Describe the operation of the Plan-Do-Check-Act model
3.1.2 Explain the need for leadership of the information risk management programme
3.1.3 Explain the need for an information risk management policy
3.1.4 Explain the need for responsibility and accountability
3.1.5 Explain the need for the integration of information risk management into business-as-usual operations
3.1.6 Explain the need for proper assignment of resources to undertake an information risk management programme
3.1.7 Explain the need for regular communications and reporting

3.2 Development of the strategic approach to information risk management

3.2.1 Explain the need to establish both the internal and external contexts in which the organisation operates and the context of the information risk management process
3.2.2 Outline the requirement to define the organisation’s risk appetite and the criteria for risk acceptance
3.2.3 Outline the requirement to verify the organisation’s information assurance requirements
3.2.4 Outline the requirement to verify the organisation’s legal and regulatory requirements
3.2.5 Describe the need to ensure communications and consultation between stakeholders at all levels
3.2.6 Explain the need to set the scope of the information risk management programme

3.3 Information classification

3.3.1 Explain the need for and purpose of a classification scheme for information assets
3.3.2 Explain the process for identifying and documenting information assets and their owners
3.3.3 Describe the use of confidentiality, integrity and availability in the development of an information classification scheme
3.3.4 Explain the requirements for a periodic review of information and its classifications
3.3.5 Describe the main differences between various classifications such as – strictly confidential; confidential; unclassified
3.3.6 Understand the differences between information classification, privacy marking and handling caveats.
4 Risk identification (9 hours)

This section of the syllabus examines the first part of the information risk management programme, and deals in greater detail with the identification of information risk.

4.1 Identification of assets

4.1.1 Describe various types of both tangible and intangible information assets

4.2 Business impact analysis

4.2.1 Outline who should be involved in a business impact analysis
4.2.2 Describe how to formulate business interruption costs in terms of confidentiality, integrity and availability
4.2.3 Explain the uses of cost of failure analyses
4.2.4 Explain how to formulate business interruption costs in terms of confidentiality, integrity and availability
4.2.5 Explain the difference between direct and indirect impacts
4.2.6 Explain the difference between primary and secondary impacts and the possibility of new impacts or vulnerabilities being introduced as a result of treating risks
4.2.7 Outline how scales may be used to quantify impact levels

4.3 Threat and vulnerability assessment

4.3.1 Describe the most common threats and hazards and explain the difference between them
4.3.2 Outline the possible motivations for threats and the likely individuals or organisations that might cause them
4.3.3 Describe the most common vulnerabilities
4.3.4 Explain the difference between likelihood and probability
4.3.5 Outline how scales may be used to quantify likelihood levels
4.3.6 Explain the use of statistical or historic data to predict likelihood
5 Risk assessment (8 hours)

This section of the syllabus deals with how risks are analysed and evaluated, how the results are recorded and prioritised and how appropriate controls may be selected.

5.1 Risk analysis

5.1.1 Explain the differences between, and the appropriate use of qualitative and quantitative risk analysis
5.1.2 Explain the difference between generic and specific risk analyses
5.1.2 Describe the construction and use of a risk matrix
5.1.3 Explain how to specify suitable impact, proximity and likelihood scales
5.1.4 Explain the concept of risk as an opportunity

5.2 Risk evaluation

5.2.1 Explain how to quantify the results of a risk assessment
5.2.2 Describe the process for comparing the results of the risk analysis with the organisation’s risk criteria and risk appetite
5.2.4 Explain the purpose and probable contents of a risk register

6 Risk treatment (2 hours)

This section of the syllabus covers the risk treatment process

6.1 Risk treatment options, controls and processes

6.1.1 Describe the four strategic risk treatment options – risk avoidance or termination; risk reduction or modification; risk transference or sharing; risk acceptance or toleration and risk retention
6.1.2 Describe the purpose of tactical risk treatment controls – prevention; detection; correction; direction; elimination; impact minimisation, monitoring and awareness, deterrence and recovery.
6.1.3 Describe the three types of operational risk treatment controls – procedural/people; physical/environmental and technical/logical
6.1.4 Explain the risk treatment process, including the importance of using both strategic and tactical approaches to risk treatment
6.1.5 Explain the concepts of business continuity and disaster recovery as additional methods of treating information risk

6.2 Risk treatment plans

6.2.1 Explain the requirements for the management of a plan to treat the risks identified
7  Presenting risks and business case (2 hours)

This section of the syllabus covers the process for reporting and presenting the results of the risk assessment process and for gaining senior management approval to apply the appropriate controls.

7.1  Risk reporting and presentation

7.1.1  Explain the requirements for reporting on an information risk management programme

7.2  Business case

7.2.1  Explain the need for a business case
7.2.2  Describe the business case preparation process and format
7.2.3  Presentation for an Outline business case

8  Monitor and review (2 hours)

8.1  Information risk monitoring

8.1.1  Explain the need for monitoring of risks after treatment to ensure that the treatment has been effective
8.1.2  Explain the need to monitor methods of risk treatment to ensure that new methods of control are considered in ongoing information risk management work

8.2  Information risk review

8.2.1  Explain the need to review all risks at intervals and when either their impact or likelihood may have changed
8.2.2  Explain the need to identify new risks that might have arisen in addition to reviewing previously identified risks
8.2.3  Describe a process for ongoing reporting of the information risk management status
Levels of Skills and Knowledge / SFIA Levels

The course will provide candidates with the levels of difficulty, knowledge and skill highlighted within the following table, enabling them to develop the skills to operate at the levels of responsibility indicated. The levels of knowledge and SFIA levels are explained on the website www.bcs.org/levels.

<table>
<thead>
<tr>
<th>Level</th>
<th>Levels of Knowledge</th>
<th>Levels of Skill and Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td></td>
<td>Set strategy, inspire and mobilise</td>
</tr>
<tr>
<td>6</td>
<td>Evaluate</td>
<td>Initiate and influence</td>
</tr>
<tr>
<td>5</td>
<td>Synthesise</td>
<td>Ensure and advise</td>
</tr>
<tr>
<td>4</td>
<td>Analyse</td>
<td>Enable</td>
</tr>
<tr>
<td>3</td>
<td>Apply</td>
<td>Apply</td>
</tr>
<tr>
<td>2</td>
<td>Understand</td>
<td>Assist</td>
</tr>
<tr>
<td>1</td>
<td>Remember</td>
<td>Follow</td>
</tr>
</tbody>
</table>

Format of the Examination

<table>
<thead>
<tr>
<th>Type</th>
<th>Written Examination, 10 multiple choice questions, 6 short answer questions and 3 essay style questions (all compulsory).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duration</td>
<td>3 Hours. An additional 45 minutes will be allowed for candidates sitting the examination in a language that is not their native/mother tongue</td>
</tr>
<tr>
<td>Pre-requisites</td>
<td>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 BCS Certificate in Information Management Principles prior to sitting the PCIRM exam.</td>
</tr>
<tr>
<td>Supervised / Invigilated</td>
<td>Yes</td>
</tr>
<tr>
<td>Closed Book</td>
<td>No reading materials allowed into the examination room</td>
</tr>
<tr>
<td>Pass Mark</td>
<td>65/100 (65%)</td>
</tr>
<tr>
<td>Distinction Mark</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Delivery</td>
<td>Paper based examination only via an BCS Accredited Training Organisation</td>
</tr>
<tr>
<td>Learning Hours</td>
<td>36 hours</td>
</tr>
</tbody>
</table>

Trainer Criteria

- Hold the BCS Information Risk Management Certificate
- Have 10 days training experience or hold a train the trainer qualification
- Have a minimum of 3 years practical experience in Information Risk Management and the relevant standards

Classroom Size

| Trainer to candidate ratio | 1:16 ratio |
### Recommended Reading List

<table>
<thead>
<tr>
<th>Title</th>
<th>Authors</th>
<th>Publisher</th>
<th>Publication Date</th>
<th>ISBN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principles of Data Management</td>
<td>Keith Gordon</td>
<td>BCS Shop</td>
<td>November 2013</td>
<td>9781780171845</td>
</tr>
<tr>
<td>Governance of IT – An Executive Guide to ISO/IEC 38500</td>
<td>A L Holt</td>
<td>BCS Shop</td>
<td>September 2013</td>
<td>9781780171548</td>
</tr>
<tr>
<td>Professional Issues in IT</td>
<td>Frank Bott</td>
<td>BCS Shop</td>
<td>January 2014</td>
<td>9781780171807</td>
</tr>
<tr>
<td>Enterprise Content Management</td>
<td>Stephen A. Cameron</td>
<td>BCS Shop</td>
<td>May 2011 – 2nd Edition</td>
<td>9781906124670</td>
</tr>
</tbody>
</table>
Information Risk Management Standards

A number of standards have been developed worldwide which aim to assist organisations to implement risk management systematically and effectively.

The different standards reflect the different motivations and technical focus of their developers and may be appropriate for different organisations and situations. Standards are normally voluntary, although adherence to a standard may be required by regulators or by contract.

Commonly used standards include:

- **The Risk Management Standard**
- **COSO 2004** – Enterprise Risk Management Integrated Framework (due to be updated in 2015)
- **OCEG Red Book 2009** A Governance, Risk and Compliance Capability Model
- **ISO 27001:2013** A specification for an information security management system
- **BS 31100:2011**