BCS PRACTITIONER CERTIFICATE

INFORMATION RISK MANAGEMENT

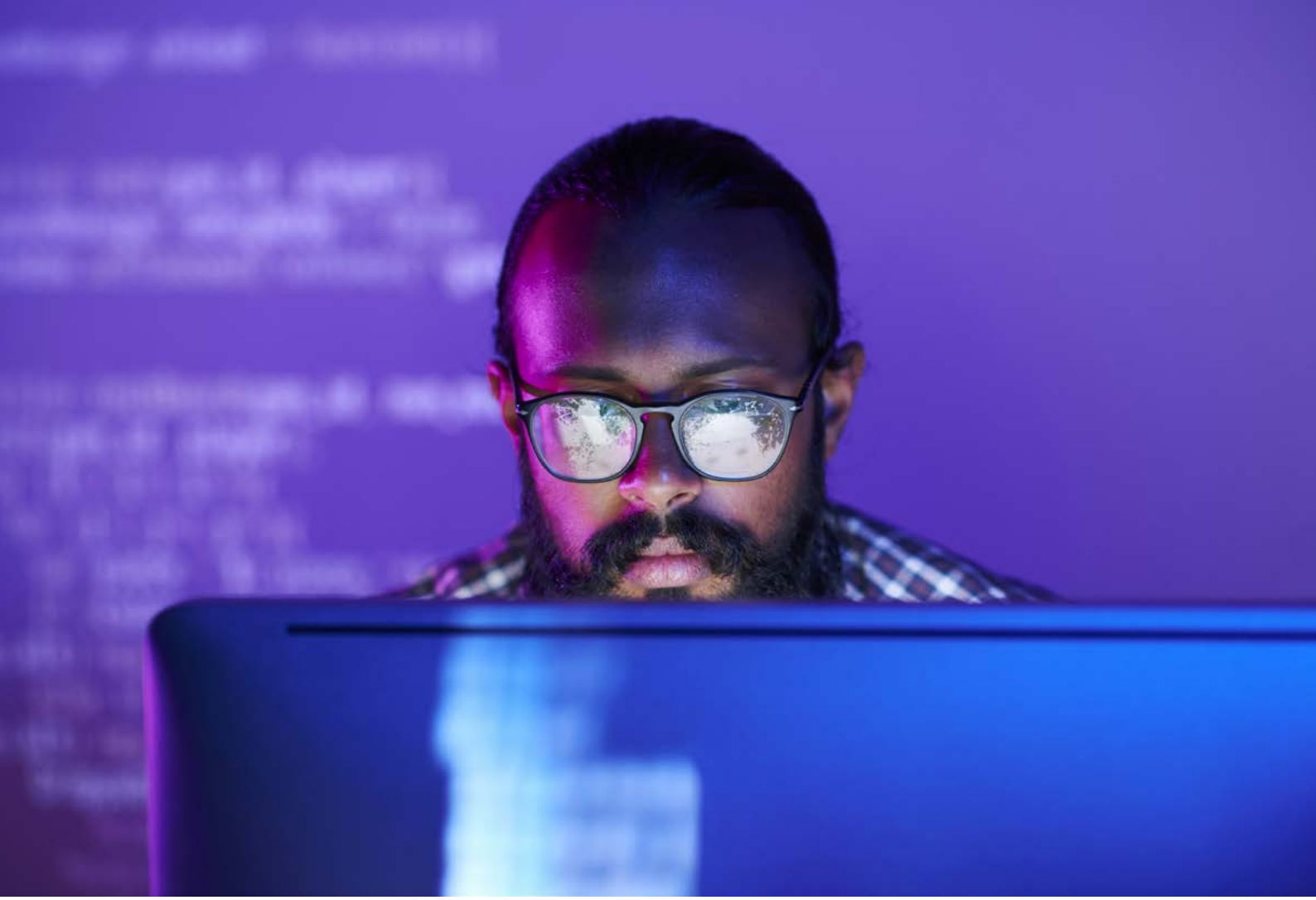
SYLLABUS

bcs
The Chartered Institute for IT

July 2022 v7.1

This is a United Kingdom government regulated qualification which is administered and approved by one or more of the following: Ofqual, Qualifications Wales, CCEA Regulation or SQA.

CONTENTS



Introduction

Every day, organisations generate and use vast amounts of data and information that can often be the target of cyber attacks. Whether it is financial information, customer or employee details, or any other information that relates to an orgnisation's activities and its stakeholders, it is critical that information is carefully managed in order to minimise the risk of it being inappropriately shared orvulnerable cyber attacks, resulting in damage to businesses or individuals.

As such, it is essential for organisations to make sure that they have the right systems, policies and procedures in place, as well as employees who are able to identify and analyse potential vulnerabilities, selecting suitable and effective approaches to manage the associated risk as part of a risk management programme.

This certificate covers the range of concepts, approaches and techniques used in information management. It promotes a hands-on approach to information risk management, using current standards and enabling candidates to make immediate use of the module content in their own context.

Candidates will be required to demonstrate their knowledge and practical application of these concepts by undertaking a scenario-based online assessment.

Qualification Suitability and Overview

There are no mandatory requirements for candidates to be able to undertake this certificate qualification, although candidates will need a good standard of written English. It will be advantageous for candidates to have an understanding of the laws that affect information risk management such as the Data Protection or Freedom of Information regulation.

This qualification has been designed for Information Risk Managers and all those who have responsibility for managing information, whether in the public or the private sector.

Candidates can study for this certificate by attending a training course provided by a BCS accredited Training Provider or through self-study.

Total Qualification Time	Guided Learning Hours	Independent Learning	Assessment Time
56 hours	**40 hours**	**16 hours**	**1.5 hours**

* Examples of Independent Learning include reading of articles or books, watching videos, attendance of other types of training or work shadowing.

Trainer Criteria

It is recommended that to effectively deliver this award, trainers should possess:

- 1 year training experience
- An Information Risk Management or similar qualification
- 1 year experience working in an information risk management role in any business area or the ability through experience to contextualise.

SFIA Levels

This award provides candidates with the level of knowledge highlighted within the table, enabling candidates to develop the skills to operate successfully at the levels of responsibility indicated.

Level	Levels of Knowledge	Levels of Skill and Responsibility (SFIA)
K7		Set strategy, inspire and mobilise
K6	Evaluate	Initiate and influence
K5	Synthesise	Ensure and advise
K4	Analyse	Enable
K3	**Apply**	**Apply**
K2	**Understand**	**Assist**
K1	**Remember**	**Follow**

SFIA Plus

This syllabus has been linked to the SFIA knowledge skills and behaviours required at level 3 for an individual working in information risk management.

KSD 21 – Familiar with Risk Management - Methods and techniques for the assessment and management of business risk including safety-related risk. Example, but not limited to: CRAMM and ISO/IEC31010 - risk management and assessment techniques.

KSD 11 – Familiar with legislation - Relevant national and international legislation. Examples, but not limited to: GDPR (General Data Protection Act) and The Computer Misuse Act. For certain industries specific legislation requires conformance to the destruction of information and also the recording and safe transfer and storage of data for a defined period of time.

KSCA2 – Proficient in Infrastructure/ system security - The security threats and vulnerabilities that impact and/or emanate from system hardware, software and other infrastructure components, and relevant strategies, controls and activities to prevent, mitigate, detect and resolve security incidents affecting system hardware, software and other infrastructure components.

KSD25 – Familiar with report writing techniques - Methods and techniques for writing clear, accessible and persuasive business and technical reports.

KSB01 – Analytical thinking - Acquiring a proper understanding of a problem or situation by breaking it down systematically into its component parts and identifying the relationships between these parts. Selecting the appropriate method/tool to resolve the problem and reflecting critically on the result, so that what is learnt is identified and assimilated.

KSB17 – Attention to detail - Applying specific quality standards to all tasks undertaken to ensure that deliverables are accurate and complete.

KSB04 – Information Acquisition - Identifying gaps in the available information required to understand a problem or situation and devising a means of resolving them.

KSC 19 – Familiar with corporate, industry and professional standards

Applying standards, practices, codes, and assessment and certification programmes relevant to the IT industry and the specific organisation or business domain

KSC24 – Aware of IT audit - Principles, practices, tools and techniques of IT auditing.

KSCA3 – Aware of Information Architecture - Methods, techniques and technologies for ingesting, securing, processing and using data and information within and beyond an organisation.

Further detail around the SFIA Levels can be found at www.bcs.org/levels.

Learning Outcomes

Upon completion of this module, candidates will be able to demonstrate:

- Knowledge and understanding of information risk management principles and techniques.
- An understanding of how the management of information risk will bring about significant business benefits.
- An understanding of how to explain and make full use of information risk management terminology.
- A practical understanding of how to conduct threat and vulnerability assessments, business impact analyses and risk assessments.
- A practical understanding of the principles of controls and risk treatment.
- A practical understanding of the use of information classification schemes.
- A practical understanding of how to present the results in a format which will form the basis of a business case for a risk treatment plan.

Syllabus

1. The concepts and framework of information risk management (5%, K2)

Candidates will be able to:

1.1 Explain the need for information risk management.

Indicative content

a. The lifecycle of information.
b. What information risk management is, and why and when it should be undertaken.
c. Which parts of an organisation may practice information risk management.
d. The general legal and regulatory framework that surrounds risks to information.

Guidance

Before exploring the detail of the information risk management process, candidates need to understand the what, why, when and where of information, and to be aware of such legal and regulatory instruments that exist to ensure its protection. Note: Specific legal and regulatory frameworks will be discussed in more detail in section 2. It should be recognised that these legal and regulatory frameworks may differ based on geographical location and industry.

1.2 Explain the context of risk in organisations.

Indicative content

a. Why organisations must take account of information risk.
b. The benefits to organisations of undertaking information risk management.
c. The potential consequences to organisations of not undertaking information risk management.

Guidance

Candidates should have an awareness of how organisations can benefit from information risk management.

2. Information risk management fundamentals (10%, K2)

Candidates will be able to:

2.1 Explain the fundamentals of information security.

Indicative content

a. The concepts of confidentiality, integrity, availability (CIA).
b. The concepts of accountability, non-repudiation, authenticity, privacy, secrecy, identification, resilience and reliability.
c. The differences between information security, cyber security, information risk management and information assurance.

Guidance

It is important that candidates clearly understand not only the concepts used in the context of information, but also the particular similarities and differences between the higher-level topics. ISO Guide 73:2009 Standard covers most terminology, however, some definitions are available from other sources.

2.2 Explain information risk management standards and good practice guides.

Indicative content

a. The need for and the uses of international information risk management standards.
b. Various standards that apply to information risk management, including ISO Guide 73:2009, ISO 27001:2017 , ISO 27005:2018 , ISO 31000:2018 and BS 31100:2011.
c. The need to understand the national legal and regulatory environment.
d. Various legal and regulatory instruments, such as the Data Protection Act and the General Data Protection Regulations, the Official Secrets Act, the Freedom of Information Act, or the PCI Data Security Standard.
e. Information available from professional organisations such as the Institute of Risk Management and the Business Continuity Institute.

Guidance

Candidates should be aware that there are a number of pieces of legislation and codes of practice of which they should have an understanding of and be able to apply when handling different types of requests for information. They do not need to know each piece of legislation in depth (and some listed in this syllabus will be more relevant to different countries, organisations and sectors) however having a basic understanding of the principles of various regulations, codes of practice and legislation and in which circumstances they apply is important when undertaking an information risk management exercise.

2.3 Explain the process of information risk management.

Indicative content

a. The overall process of risk management.
b. The concept of information risk ownership.
c. The four stages of information risk management, covering context establishment; risk assessment; (risk identification, risk analysis, risk evaluation and risk treatment); communication and consultation; and monitoring and review.
d. Risk management methodologies.

Guidance

Candidates should have a thorough understanding of the process for managing information risk (which is detailed in further sections of this syllabus), and also of the concept of information risk ownership, which may be different from ownership of the information itself. Also, there exists a number of commercial risk management methodologies, and whilst candidates are not required to have a detailed knowledge of these, they should have a basic appreciation, so that a suitable methodology can be selected.

2.4 Explain information risk terms and definitions.

Indicative content

a. The meaning of the terms threats, hazards, vulnerabilities, proximity, likelihood, probability and risk.
b. The strategic risk treatment options, including risk avoidance or termination; risk reduction or modification; risk transference or sharing; risk acceptance or tolerance and risk retention.
c. The choices of tactical risk controls, including preventative, detective, directive and corrective.
d. The selection of operational risk controls, including physical or environmental, technical or logical and procedural or people.

Guidance

In order to fully engage with information risk management, candidates must have an in-depth understanding of strategic, tactical and operational controls. Understanding the different types should allow them to select the most appropriate combination of controls. The option of doing nothing or ignoring risks must be avoided at all costs.

3. Establishing an information risk management programme (12%, K2)

Candidates will be able to:

3.1 Understand the requirements of an information risk management programme.

Indicative content

a. The Plan-Do-Check-Act model, also known as the Deming Cycle.
b. Leadership of the information risk management programme.
c. An information risk management policy
d. Responsibility and accountability.
e. The integration of information risk management into business-as-usual operations.
f. The proper assignment of resources to undertake an information risk management programme.
g. Regular communications and reporting.

Guidance

In order to prepare for an information risk management programme, candidates should have a solid appreciation of how to approach and construct such a programme. In particular, candidates should consider carefully who should participate in the programme, and in what role.

3.2 Explain the development of a strategic approach to information risk management.

Indicative content

a. Establishing both the internal and external contexts in which the organisation operates and the context of the information risk management process.
b. Definitions of an organisation's overall risk appetite, its individual risk tolerance and its criteria for risk acceptance.
c. Verification of the organisation's information assurance requirements.
d. Verification of the organisation's legal and regulatory requirements.
e. Ensuring communications and consultation between stakeholders at all levels.
f. Setting the scope of the information risk management programme.

Guidance

Candidates will need to have a full understanding and appreciation of how their organisation operates, its goals and objectives, its environment, and the financial, political and commercial constraints it faces. It will be critical to the success of the information risk management programme for candidates to understand and be able to communicate with stakeholders at all levels.

3.3 Explain the principles of information classification.

Indicative content

a. The requirement for and purpose of a classification scheme for information assets.
b. Identifying and documenting information assets and their owners.
c. The use of confidentiality, integrity and availability in the development of an information classification scheme.
d. Periodic reviews of information and its classifications.
e. Types of classification such as strictly confidential; confidential; unclassified.
f. The difference between information classification, privacy marking and handling caveats.

Guidance

Appropriate information classification is key to a successful information risk management programme, since it will define which aspects of the organisation's information must be protected, to what degree, and the means by which its assets are protected. Some knowledge of aggregation of data and how it may impact information classification is useful,

4. Risk identification (21%, K3)

Candidates will be able to:

4.1 Describe the process to identify information assets.

Indicative content

a. Examples of both tangible and intangible information assets.

Guidance

Candidates should be able to identify all forms of an organisation's information, regardless of its type. Tangible assets are those that may be stored as electronic files, film, photographs, audio recordings or paper copy information, and all such types of information will form an organisation's information assets. Intangible assets include such things as reputation, patents, copyrights and trademarks.

4.2 Conduct a business impact analysis.

Indicative content

a. The overall business impact analysis process, and who should be involved in it.
b. How to formulate business interruption costs in terms of confidentiality, integrity and availability.
c. The uses of cost of failure analyses.
d. The concept of worst-case scenarios.
e. The difference between direct and indirect impacts.
f. The difference between primary and secondary impacts and the possibility of new impacts or vulnerabilities being introduced as a result of treating risks.
g. How scales may be used to quantify impact levels.

Guidance

Candidates should have an in-depth understanding of the overall business impact analysis process, since this will form the basis of all other information risk management work. This will involve the use of quantitative (numerically measurable) assessments, qualitative (e.g. low, medium and high) assessments, and of semi-quantitative assessments, where the impacts assessed will fall into numerical layers (e.g. low is between zero and £100,000).

4.3 Conduct a threat and vulnerability assessment.

Indicative content

a. How threats and likelihood combine to create a risk.
b. The most common threats and hazards and explain the difference between them.
c. Possible motivations for threats and the likely individuals or organisations that might cause them.
d. The most common vulnerabilities.
e. The difference between likelihood and probability.
f. How scales may be used to quantify likelihood levels.
g. The use of statistical or historic data to predict likelihood.

Guidance

Having assessed the business impacts on information assets, candidates must understand the process of assessing the threats and hazards these assets face, and the likelihood or probability that one or more threat or hazard will actually occur, causing the impact already assessed.

As with impact assessments, this will involve the use of quantitative (numerically measurable) assessments, qualitative (e.g. low, medium and high) assessments, and of semi-quantitative assessments, where the likelihood or probability assessed will fall into numerical layers (e.g. low is between zero and 25 percent).

5. Risk assessment (21%, K3)

Candidates will be able to:

5.1 Undertake a risk analysis

Indicative content

a. The differences between, and the appropriate use of qualitative, quantitative and semi-qualitative risk analysis.
b. The difference between generic and specific risk analyses.
c. The construction and use of a risk matrix.
d. How to specify suitable impact, proximity and likelihood scales.
e. The concept of risk as an opportunity.

Guidance

Having assessed the impacts, potential threats or hazards and likelihood or probability, candidates will now be able to conduct a risk assessment, and present the results in the form of a risk matrix which will illustrate visually the severity of each impact. Candidates will also gain an appreciation of how best to construct the risk matrix in order to avoid too many impacts being grouped in any one area.

5.2 Conduct risk evaluation.

Indicative content

a. How to quantify the results of a risk assessment.
b. The process for comparing the results of the risk analysis with the organisation's risk criteria and risk appetite.
c. The purpose and probable contents of a risk register.

Guidance

The final part of the risk assessment process is to prioritise the individual impacts (or groups of impacts) in terms of their need for treatment – the most serious of which should always be treated before the lesser impacts.

6. Risk treatment (19%, K2)

Candidates will be able to:

6.1 Explain risk treatment options, controls and processes.

Indicative content

a. 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.
b. The purpose of tactical risk treatment controls - prevention; detection; correction; direction; elimination; impact minimisation, monitoring and awareness, deterrence and recovery.
c. The three types of operational risk treatment controls - procedural/people; physical/environmental and technical/logical.
d. The risk treatment process, including the importance of using a combination of strategic, tactical and operational approaches to risk treatment.
e. The concepts of resilience, business continuity and disaster recovery as additional methods of treating information risk.

Guidance

Having identified and prioritised the various impacts, candidates may now commence drawing up the plan to treat them. This will involve a number of choices at strategic, tactical and operational levels in order to ensure that the risks are either eliminated completely, or reduced as far as possible.
It will become clear to candidates that treatment of individual risks may not always involve a single activity, but may well require multiple activities at different strategic, tactical and operational levels.

6.2 Explain the use of a risk treatment plan.

Indicative content

a. Requirements for the management of a plan to treat the risks identified.

Guidance

Once the individual or group risk treatments have been identified and verified with their risk owners and asset owners, candidates will need to prepare an overall plan of how and when to carry out the treatment activities, bearing in mind not only priorities, but also the financial costs of doing so and the resources required.

Naturally, the activities involved in treating the risks will require additional input from the people responsible for undertaking them in order to ensure that resource conflicts are avoided.

7. Monitor and review (6%, K3)

Candidates will be able to:

7.1 Explain information risk monitoring.

Indicative content

a. The need for monitoring of risks after treatment to ensure that the treatment has been effective.
b. The need to monitor methods of risk treatment to ensure that new methods of control are considered in ongoing information risk management work.

Guidance

Candidates should understand that once a risk has been treated, that activity may not indicate the end of the matter. It will be clear that a risk that has been treated must be monitored to verify the success of the treatment option, and that unless the risk has been completely negated, that ongoing monitoring will be required. The more established methods of treatment must also be monitored, since changes in processes and technology may render some forms of treatment redundant, and that new and different forms of treatment may be required.

7.2 Undertake an information risk review.

Indicative content

a. The need to review all risks at intervals and when either their impact or likelihood may have changed.
b. The need to identify new threats that may have arisen, and therefore to identify new risks that might have arisen in addition to reviewing previously identified risks.
c. How new threats can be identified i.e. through the sources available, forums, other resources.
d. A process for ongoing reporting of the information risk management status.

Guidance

It will also be clear that information risk management requires that periodic reviews of the organisation's information assets will be required to identify any new risks that have developed over time. This will require a review for each information asset as to whether its impact has changed, an exercise to identify new assets, and possible new threats or hazards.
Finally, candidates should understand the need to report the output of these reviews to the appropriate levels within the organisation.

8. Presenting risks and business case (6%, K4)

Candidates will be able to:

8.1 Report and present the progress of a risk management programme.

Indicative content

a. The requirements for reporting on an information risk management programme.
b. The possible contents of a risk report.

Guidance

One of the key activities that candidates will need to undertake is the preparation and presentation of a risk management programme which will detail the risks that have been identified together with their potential severity, that proposed method of treating them, the costs and timescales involved, and what residual risk (if any) will remain.

8.2 Present a business case

Indicative content

a. The need for a business case.
b. Business case preparation process and format.
c. Presentation of an outline business case.

Guidance

In order to present a business case (often to Board level) candidates must be well-prepared, having produced a clear and comprehensive report, and be able to format their presentation so that the recipients are not overloaded with information, which can be easily understood by non-technical people, and must finish with the recommendations and decisions they are required to make in order for the risk treatment plan to move forward.
Candidates may find that undertaking presentation skills training will be to their advantage in undertaking business case presentations

Examination Format

This certificate is assessed through completion of an invigilated online exam which candidates will only be able to access at the date and time they are registered to attend.

Type	A scenario-based online exam that includes a range of question types including multiple choice, multiple response, and matching questions.
Duration	90 minutes
Supervised	Yes
Open Book	No (no materials can be taken into the examination room)
Passmark	39/60 (65%)
Delivery	Digital format only.

Adjustments and/or additional time can be requested in line with the BCS reasonable adjustments policy for candidates with a disability, or other special considerations including English as a second language.

Question Weighting

Each major subject heading in this syllabus is assigned a percentage weighting. The purpose of this is:

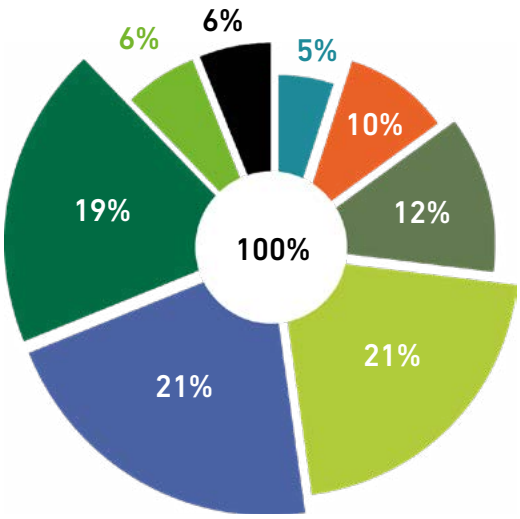
1. Guidance on the proportion of content allocated to each topic area of an accredited course.
2. Guidance on the proportion of questions or marks in the exam.

Syllabus Area

1. The concepts and framework of information risk management	**5%**
2. Information risk management fundamentals	**10%**
3. Establishing an information risk management programme	**12%**
4. Risk identification	**21%**
5. Risk assessment	**21%**
6. Risk treatment	**19%**
7. Monitor and review	**6%**
8. Presenting risks and business case	**6%**

Question types

A mix of question types will be used including multiple choice , multiple response, fill in the blanks, ordering and matching



Syllabus Weighting

Recommended Reading

The following resources and titles are suggested reading for anyone undertaking this award. Candidates should be encouraged to explore other available sources.

Books

Title	Information Risk Management: A Practitioner's Guide
Authors	David Sutton
Publisher	BCS, Learning and Development Limited
Publication Date	November 2014 (Second edition due for publication in late 2021)
ISBN	978-1-78017-265-1

Title	Information Security Management Principles
Authors	David Alexander, Amanda Finch, David Sutton, Andy Taylor
Publisher	BCS, Learning and Development Limited
Publication Date	January 2020 - 3rd edition
ISBN	978-1-78017-518-8

Legislation

Data Protection Act 2018. Her Majesty's Stationery Office.	https://www.gov.uk/government/collections/data-protection-act-2018
The General Data Protection Regulation (GDPR).	https://ec.europa.eu/info/law/law-topic/data-protection_en
The Computer Misuse Act 1990. Her Majesty's Stationery Office.	http://www.legislation.gov.uk/ukpga/1990/18/contents
The Police and Criminal Evidence Act 1984. Her Majesty's Stationery Office.	http://www.legislation.gov.uk/ukpga/1984/60/contents
The Official Secrets Act 1989. Her Majesty's Stationery Office.	http://www.legislation.gov.uk/ukpga/1989/6/contents
The Freedom of Information Act 2000. Her Majesty's Stationery Office.	http://www.legislation.gov.uk/ukpga/2000/36/contents

The Regulation of Investigatory Powers Act 2000. Her Majesty's Stationery Office.	http://www.legislation.gov.uk/ukpga/2000/23/contents
The Copyright, Designs and Patents Act 1988. Her Majesty's Stationery Office.	http://www.legislation.gov.uk/ukpga/1988/48/contents
Control Of Major Accident Hazards Regulations 2015. Health and Safety Executive	http://www.legislation.gov.uk/uksi/2015/483/contents/made
Civil Contingencies Act 2004. Her Majesty's Stationery Office.	http://www.legislation.gov.uk/ukpga/2004/36/contents

Codes of Practice

Good Practice Guidelines 2018. The Business Continuity Institute.	https://www.thebci.org/training-qualifications/good-practice-guidelines.html

Guidance

The Traffic Light Protocol (TLP). European Network and Information Security Agency (ENISA).	https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/considerations-on-the-traffic-light-protocol
The Capability Maturity Model. Carnegie Mellon University.	https://www.itgovernance.co.uk/capability-maturity-model
Critical Security Controls Version 7.1. The Centre for Internet Security.	https://cybernetsecurity.com/industry-papers/CIS-Controls%20Version-7-cc-FINAL.PDF
The IISP Skills Framework. The Chartered Institute of Information Security (CIISec).	https://www.ciisec.org/Skills_Framework
The IISP Knowledge Framework. The Chartered Institute of Information Security (CIISec).	https://www.ciisec.org/Knowledge_Framework
The IISP Roles Framework. The Chartered Institute of Information Security (CIISec).	https://www.ciisec.org/Roles_Framework

A Structured Approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000. The Federation of European Risk Management Associations (FERMA).	https://www.ferma.eu/app/uploads/2011/10/a-structured-approach-to-erm.pdf
The Standard for Information Assurance for Small and Medium Sized Enterprises (IASME).	https://iasme.co.uk

Websites

HMG Cyber Essentials Scheme from the Department for Digital, Culture, Media & Sport (DCMS).	https://www.gov.uk/government/publications/cyber-essentials-scheme-overview
10 Steps to Cyber Security, produced by the National Cyber Security Centre (NCSC).	https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security
CORAS Risk Assessment Platform. SourceForge	http://coras.sourceforge.net/index.html
FAIR (Factor Analysis of Information Risk). Risk Management Insight.	https://www.fairinstitute.org

The OCTAVE Method (Operationally Critical Threat, Asset, and Vulnerability Evaluation).

The OCTAVE-S Method – designed for use by smaller organisations.

The OCTAVE Allegro Method, a streamlined approach for information security assessment and assurance. Carnegie Mellon University.

Details of all three Octave methodologies are available from the Carnegie Mellon University:	https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=309051
SABSA (Sherwood Applied Business Security Architecture). The SABSA Institute.	http://www.sabsa.org/

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:

- ISO 31000:2018 - Risk Management Principles and Guidelines
- The Risk Management Standard
- ISO31010:2019 - Risk Management - Risk Assessment Techniques
- COSO 2017 - Enterprise Risk Management Integrated Framework (due to be updated in 2015)
- OCEG Red Book 2009 A Governance, Risk and Compliance Capability Model
- ISO Guide 73:2009 Definitions of generic terms related to Risk Management.
- ISO 27005:2018 Guidelines for information security risk management.
- ISO 27001:2017 A specification for an information security management system
- BS 31100:2011

ISO Standards are available for purchase from.	https://www.iso.org/store.html or https://shop.bsigroup.com/
The Risk Management Standard can be downloaded from	https://www.theirm.org/what-we-do/what-is-enterprise-risk-management/irms-risk-management-standard/
The COSO Enterprise Risk Management document can be obtained from	https://www.coso.org/pages/erm-integratedframework.aspx
The OCEG Capability Model can be downloaded from	https://go.oceg.org/grc-capability-model-red-book (registration is required)
The BS 31100:2011 Standard may be purchased from	https://shop.bsigroup.com/

Using BCS Books

Accredited 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 request a licence, please contact the Head of Publishing at BCS outlining the material you wish to copy and the use to which it will be put.

Document 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.

Version Number	Changes Made
Version 7.0 May 2021	Document Creation
Version 7.1 July 2022	Updated exam pass mark

CONTACT

For further information please contact:

BCS
The Chartered Institute for IT
3 Newbridge Square
Swindon
SN1 1BY

T +44 (0)1793 417 445

www.bcs.org

© 2021 Reserved. BCS, The Chartered Institute for IT

All rights reserved. No part of this material protected by this copyright may be reproduced or utilised in any form, or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system without prior authorisation and credit to BCS, The Chartered Institute for IT.

Although BCS, The Chartered Institute for IT has used reasonable endeavours in compiling the document it does not guarantee nor shall it be responsible for reliance upon the contents of the document and shall not be liable for any false, inaccurate or incomplete information. Any reliance placed upon the contents by the reader is at the reader's sole risk and BCS, The Chartered Institute for IT shall not be liable for any consequences of such reliance.

The Chartered Institute for IT

Copyright © BCS 2022