IIBA CCA

IIBA CYBERSECURITY ANALYSIS CERTIFICATION QUESTIONS & ANSWERS

Exam Summary – Syllabus – Questions

CCA

IIBA Cybersecurity Analysis (CCA)

75 Questions Exam – Duration of 90 minutes

www.ProcessExam.com

Table of Contents

Know Your CCA Certification Well:

The CCA is best suitable for candidates who want to gain knowledge in the IIBA Cybersecurity. Before you start your CCA preparation you may struggle to get all the crucial Cybersecurity Analysis materials like CCA syllabus, sample questions, study guide.

But don't worry the CCA PDF is here to help you prepare in a stress free manner.

The PDF is a combination of all your queries like-

- What is in the CCA syllabus?
- How many questions are there in the CCA exam?
- Which Practice test would help me to pass the CCA exam at the first attempt?

Passing the CCA exam makes you IIBA Cybersecurity Analysis (CCA). Having the Cybersecurity Analysis certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

IIBA CCA Cybersecurity Analysis Certification Details:

Exam Name	IIBA Cybersecurity Analysis
Exam Code	CCA
Exam Fee	Exam Fee: Member - $250, Non-Member - $400 Retake Fee: Member - $195, Non-Member - $350
Exam Duration	90 Minutes
Number of Questions	75
Passing Score	Pass or Fail
Format	Multiple Choice Questions
Schedule Exam	**PROMETRIC**
Sample Questions	**IIBA Cybersecurity Analysis Exam Sample Questions and Answers**
Practice Exam	**IIBA Cybersecurity Analysis (CCA) Practice Test**

CCA Syllabus:

Topic	Details	Weights
Cybersecurity Overview and Basic Concepts	- General Awareness: Understands the role of Business Analysis in Cybersecurity - Practical Knowledge: Follows Rules to conduct a stakeholder analysis - Practical Knowledge: Follows Rules using existing documentation to draft a RACI for a Cybersecurity project or program initiative - General Awareness: Understands how to locate the organization's security framework or model, or know that one does not yet exist - General Awareness: Understands what an Information Security Management System (ISMS) is and its objective - General Awareness: Understands what data privacy is - General Awareness: Understands the difference between an internal and external audit. - Practical Knowledge: Follows Rules and knows the difference between compliance and best practice	14%
Enterprise Risk	- General Awareness: Understands what a cyber risk is - General Awareness: Basic Knowledge of what a Cybersecurity Risk Assessment is - Practical Knowledge: Follows Rules for the inputs to a Business Case that BAs are typically responsible for - General Awareness: Understands what Disaster Recovery Plans and Business Continuity Plans are - Practical Knowledge: Follows Rules to develop a business process flow diagram, and identify steps along the path that present potential cybersecurity vulnerabilities	14%
Cybersecurity Risks and Controls	- General Awareness: Understands what Cybersecurity Controls are and where to find various versions - General Awareness: Understands the three attributes of secure information: confidentiality, integrity and availability - General Awareness: Understands the difference between a cyber threat and a cyber vulnerability - Practical Knowledge: Follows Rules to identify typical impacts of a cyber-attack to an organization	12%
Securing the Layers	- General Awareness: Understands that there are multiple layers of technology to protect - General Awareness: Understands what is meant by Endpoint Security	5%
Data Security	- General Awareness: Understands what Information Classification means - General Awareness: Understands what Information Categorization means - General Awareness: Understands what Data Security at Rest means - General Awareness: Understands what Data Security in Transit means	15%

Topic	Details	Weights
	- General Awareness: Understands what Encryption is - General Awareness: Understands what a Digital Signature is	
User Access Control	- Practical Knowledge: Follows Rules to set up authorization - General Awareness: Understands what authentication is - General Awareness: Understands what access control means - General Awareness: Understands what Privileged Account Management is - Practical Knowledge: Follows Rules and is familiar with key actions employees should take responsibility for to maintain security - General Awareness: Understands the principle of least privilege - Practical Knowledge: Follows Rules to elicit user access requirements	15%
Solution Delivery	- Practical Knowledge: Follows Rules to identify a Security Requirement when presented with a list of requirements - General Awareness: Understands what SaaS, IaaS and PaaS are - Practical Knowledge: Follows Rules to document a current state business process including current technology - General Awareness: Understands a target state business process for a cybersecurity initiative - Practical Knowledge: Follows Rules to map cybersecurity solution components back to security requirements	13%
Operations	- General Awareness: Understands how to create and maintain a risk log - General Awareness: Basic Knowledge of the four risk treatment options: Accept, Avoid, Transfer, Mitigate - General Awareness: Understands what residual risk is - General Awareness: Understands how to create a report template for Security metrics - General Awareness: Understands Root Cause Analysis	12%

IIBA CCA Sample Questions:

Question: 1

Examples of encryption technology controls for data in transit are:

a) information categorization and multi-factor authentication.
b) cryptographic policy management and training.
c) concurrent session control and firewalls.
d) hardware security modules and certificate authorities.

Answer: d

Question: 2

The amount of risk an organization requires to meet their goals is called:

a) risk appetite.
b) vulnerability impact.
c) risk management.
d) risk capacity.

Answer: d

Question: 3

What type of access is granted for groups of employees based on job classification and function?

a) Information Classification.
b) Role Based Access.
c) Preferred Access.
d) Shared Account.

Answer: b

Question: 4

A certificate chain is a series of certificates issued by successive 'Certificate Authorities' that trace a path of certificates

a) from the branch in the hierarchy to a leaf in the hierarchy.
b) from a leaf in the hierarchy to the branch in the hierarchy.
c) from the root in the hierarchy to a branch in the hierarchy.
d) from a branch in the hierarchy to the root of the hierarchy.

Answer: d

Question: 5

What is the difference between a policy and a standard for cybersecurity?

a) A policy defines objectives and governance; a standard describes how to implement policies through specific controls.
b) A policy is a guideline, whereas a standard must be followed.
c) Policies are internal to the enterprise; standards are mandated by external regulators.
d) Standards define what an enterprise must do, whereas policies describe how a standard is implemented.

Answer: a

Question: 6

In Security Engineering, the Business Analyst's role is to represent the enterprise-level security requirements, to ensure that:

a) the architecture and designs align with the organization's core goals and strategic direction.
b) employees are trained to recognize phishing attacks.
c) a control framework is in place.
d) an organizational risk assessment includes assets used by engineering teams.

Answer: a

Question: 7

Which principle should be followed when gathering access control requirements?

a) Principle of Least Privilege.
b) Principle of Defense in Depth.
c) Principle of Thinking Evil.
d) Principle of Simplicity.

Answer: a

Question: 8

The business case for cybersecurity support should include:

a) Assessment of potential providers and a ranking of their capabilities.
b) Implementation plans describing outsourcing arrangements.
c) Analysis of potential risks, including the probability and impact of the risk.
d) Detailed metrics that will be used to assess the performance of the selected vendor.

Answer: c

Question: 9

What risk attribute must be tracked on a Risk Log to ensure someone is held accountable for the risk?

a) Risk Response Plan.
b) Risk Owner.
c) Risk Category.
d) Risk Score.

Answer: b

Question: 10

Unchecked user input is a cause of vulnerabilities because:

a) the users may be able to exploit a bug.
b) the user may have malware installed on their computer that will be able to intercept information.
c) it may allow unintended direct execution of commands.
d) passwords may be easily guessed by outsiders.

Answer: c

Study Guide to Crack IIBA Cybersecurity Analysis CCA Exam:

- Getting details of the CCA syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the CCA exam.

- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.

- Joining the IIBA provided training for CCA exam could be of much help. If there is specific training for the exam, you can discover it from the link above.

- Read from the CCA sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.

- Practicing on CCA practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for CCA Certification

Make ProcessExam.com your best friend during your IIBA Cybersecurity Analysis exam preparation. We provide authentic practice tests for the CCA exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual CCA exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don't bother if you don't get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the CCA exam.

Start Online Practice of CCA Exam by Visiting URL

https://www.processexam.com/iiba/iiba-cybersecurity-analysis-cca