bakkah

IIBA®-CCA

Certificate in Cybersecurity Analysis

IIBA®-CCA

Training Course

Certification provided by IIBA® Endorsed Education

Why Bakkah?

Bakkah Learning is a leading company in the training field, with a team of carefully acquired experts in different spectrums of business to support learners in their journey to achieve professionalism and better opportunities in life.

CONTENT

- Designed by Experts
- Aligned with today's business world topics .

PARTNERSHIPS

- Exclusive Partnerships with International Accreditation Bodies, like IIBA.

24/7 TECHNICAL SUPPORT

- Ready to answer your inquiries and handle your requests.

FLEXIBLE DELIVERY METHODS

- Live Online

About the Course

The IIBA®-CCA course, accredited by IIBA®, equips professionals with capability assessment skills. It covers frameworks, methodologies, and best practices. Completing the course enhances credibility and prepares individuals to conduct effective assessments.

Why Earn this Badge?

Earning the IIBA®-CCA badge offers the following benefits:

01 Enhance expertise in capability assessment.

Expand career opportunities in the field. 02

03 Drive organizational improvement.

Gain industry recognition and respect. 04

05 Stay updated with industry best practices.

Who Needs this Badge?

01 Business analysts who specialize in capability assessment.

02 Consultants and advisors involved in assessing and improving organizational performance.

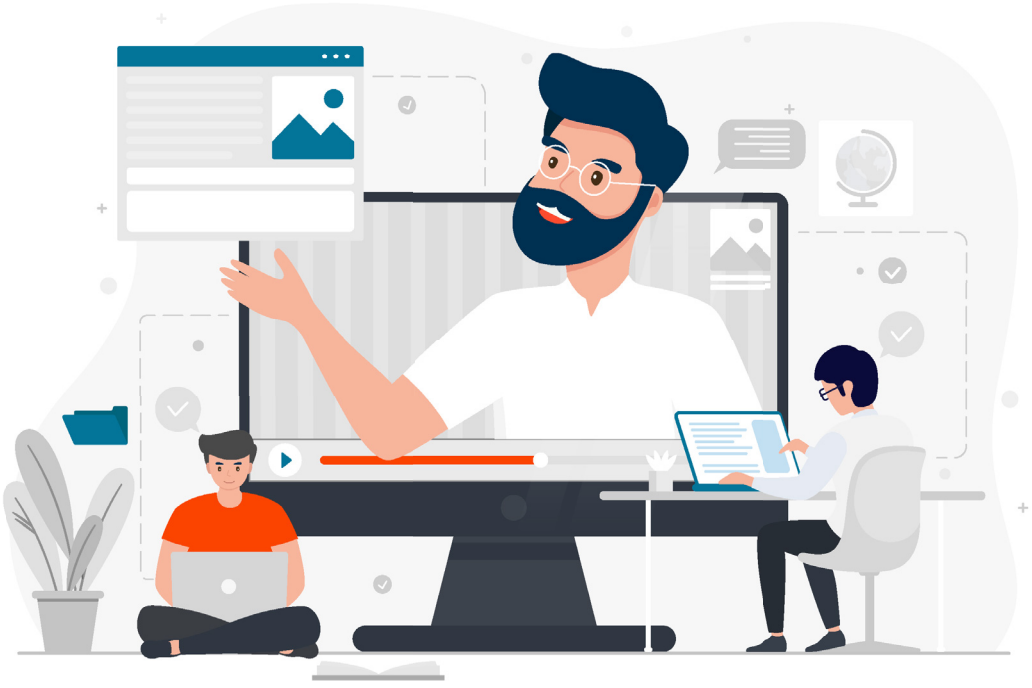
03 Process improvement specialists focused on enhancing business processes.

04 Project managers aiming to assess team or organizational capabilities.

05 Quality assurance professionals evaluating and improving organizational processes.

06 Change management specialists assessing readiness for successful transformations.

07 Organizational development practitioners aligning capabilities with strategic goals.



Course Objectives:

By the end of this course, you'll be able to:

01 Understand capability assessment concepts and principles.

02 Apply assessment methodologies to evaluate capabilities.

03 Identify organizational strengths and weaknesses.

04 Develop actionable improvement recommendations.

05 Communicate assessment findings effectively.

06 Implement change initiatives for enhanced capabilities.

07 Align capabilities with strategic objectives.

08 Contribute to continuous improvement efforts.

09 Apply industry best practices in assessment.

10 Prepare for and pass the IIBA®-CCA certification exam.

Exam Details

IIBA-CCA Certification Exam Format

- Objective testing
- 75 questions, each worth 1 mark
- 90 minutes

IIBA®-CCA Certifications

Log in or create an IIBA profile and go to My Certifications and the Certification Summary page. Review the specific handbook for details and purchase your exam.

Course Outlines

Cybersecurity Overview and Basic Concepts

- 1.1 **General Awareness:** Understands the role of Business Analysis in Cybersecurity
- 1.2 **Practical Knowledge:** Follows Rules to conduct a stakeholder analysis
- 1.3 **Practical Knowledge:** Follows Rules using existing documentation to draft a RACI for a Cybersecurity project or program initiative
- 1.4 **General Awareness:** Understands how to locate the organization›s security framework or model, or know that one does not yet exist
- 1.5 **General Awareness:** Understands what an Information Security Management System (ISMS) is and its objective
- 1.6 **General Awareness:** Understands what data privacy is
- 1.7 **General Awareness:** Understands the difference between an internal and external audit.
- 1.8 **Practical Knowledge:** Follows Rules and knows the difference between compliance and best practice

Enterprise Risk

- 2.1 **General Awareness:** Understands what a cyber risk is
- 2.2 **General Awareness:** Basic Knowledge of what a Cybersecurity Risk Assessment is
- 2.3 **Practical Knowledge:** Follows Rules for the inputs to a Business Case that BAs are typically responsible for
- 2.4 **General Awareness:** Understands what Disaster Recovery Plans and Business Continuity Plans are
- 2.5 **Practical Knowledge:** Follows Rules to develop a business process flow diagram, and identify steps along the path that present potential cybersecurity vulnerabilities

Course Outlines

Cybersecurity Risks and Controls

- 3.1 **General Awareness:** Understands what Cybersecurity Controls are and where to find various versions
- 3.2 **General Awareness:** Understands the three attributes of secure information: confidentiality, integrity and availability
- 3.3 **General Awareness:** Understands the difference between a cyber threat and a cyber vulnerability
- 3.4 **Practical Knowledge:** Follows Rules to identify typical impacts of a cyber-attack to an organization

Securing the Layers

- 4.1 **General Awareness:** Understands that there are multiple layers of technology to protect
- 4.2 **General Awareness:** Understands what is meant by Endpoint Security

Enterprise Risk

- 5.1 **Practical Knowledge:** Follows Rules to set up authorization
- 5.2 **General Awareness:** Understands what authentication is
- 5.3 **General Awareness:** Understands what access control means
- 5.4 **General Awareness:** Understands what Privileged Account Management is
- 5.5 **Practical Knowledge:** Follows Rules and is familiar with key actions employees should take responsibility for to maintain security
- 5.6 **General Awareness:** Understands the principle of least privilege
- 5.7 **Practical Knowledge:** Follows Rules to elicit user access requirements

Course Outlines

Solution Delivery

- 6.1 Practical Knowledge: Follows Rules to identify a Security Requirement when presented with a list of requirements
- 6.2 General Awareness: Understands what SaaS, IaaS and PaaS are
- 6.3 Practical Knowledge: Follows Rules to document a current state business process including current technology
- 6.4 General Awareness: Understands a target state business process for a cybersecurity initiative
- 6.5 Practical Knowledge: Follows Rules to map cybersecurity solution components back to security requirements

Operations

- 7.1 General Awareness: Understands how to create and maintain a risk log
- 7.2 General Awareness: Basic Knowledge of the four risk treatment options: Accept, Avoid, Transfer, Mitigate
- 7.3 General Awareness: Understands what residual risk is
- 7.4 General Awareness: Understands how to create a report template for Security metrics
- 7.5 General Awareness: Understands Root Cause Analysis

www.bakkah.com