bakkah

Certificate in Cybersecurity Analysis (IIBA® – CCA)

Training Course

Certification provided by IIBA® International Institute of Business Analysis™

Why Bakkah?

Bakkah is a leading company that owns two subsidiaries: **Consulting Company and Learning Company**. With a team of highly experienced and certified professionals, we will help you capitalize on opportunities driven by proven business practices.

We help you obtain professional certificates that will take your career to the next level. Our Learning products focus on building and boosting capabilities by offering the best and latest internationally accredited training courses in various fields, including: Project Management, Human Resource, Business Analysis, Information Technology, Quality Management, Supply Chain Management and Logistics.

We are keen to use and keep up with the latest global learning methods and processes. Since our training courses are flexible and aligned with the global changes, this will ensure an ongoing learning process and build high-quality capabilities.

Bakkah in Numbers

Course Objective

IIBA® and IEEE Computer Society have partnered to offer a robust learning and certification program on what business analysis professionals need to know to be prepared for today's cybersecurity challenges.

This course helps you to:

IIBA and IEEE Computer Society's program provides the credibility of a joint certification and the opportunity to learn key cybersecurity concepts and tools business analysis professionals need to demonstrate core competencies.

Course Methodology

Online Training

- 6 Days – Online Training
- Exam Simulation
- Practice Test
- Group Activity (Break-out Session) after each lesson
- Access to additional References – Glossary/ Recommended Reading/ Syllabus
- Material language will be in English

Targeted Audience

Business analysis professionals working in the cybersecurity space.

Course Outline

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

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

User Access Control

- 6.1 Practical Knowledge: Follows Rules to set up authorization
- 6.2 General Awareness: Understands what authentication is
- 6.3 General Awareness: Understands what access control means
- 6.4 General Awareness: Understands what Privileged Account Management is
- 6.5 Practical Knowledge: Follows Rules and is familiar with key actions employees should take responsibility for to maintain security
- 6.6 General Awareness: Understands the principle of least privilege
- 6.7 Practical Knowledge: Follows Rules to elicit user access requirements

Solution Delivery

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

Operations

- 8.1 General Awareness: Understands how to create and maintain a risk log
- 8.2 General Awareness: Basic Knowledge of the four risk treatment options: Accept, Avoid, Transfer, Mitigate
- 8.3 General Awareness: Understands what residual risk is
- 8.4 General Awareness: Understands how to create a report template for Security metrics
- 8.5 General Awareness: Understands Root Cause Analysis

bakkah

9 2 0 0 0 3 9 2 8
1 1 2 1 0 1 1 4 1
/BAKKAHINC
contactus@bakkah.net.sa
w w w . b a k k a h . c o m