

IIBA CCA® Exam Prep: Cybersecurity Analysis for Pros

15 – 19 November 2027
London

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

IIBA CCA® Exam Prep: Cybersecurity Analysis for Pros

Ref: 103600521_105120 **Date:** 15 – 19 November 2027 **Location:** London **Fees:** 6500 Euro

Course Overview

The Certificate in Cybersecurity Analysis IIBA-CCA is a specialized corporate training program designed to build business-focused cybersecurity analysis capabilities for professionals working in complex and risk-driven organizational environments. The course develops practical competencies that enable participants to analyze cybersecurity risks, assess business impact, and support informed decision-making at the enterprise level.

This Cybersecurity Analysis Training Course focuses on cyber risk analysis for business analysts, business analysis in cybersecurity, and risk-based cybersecurity analysis, empowering participants to translate cyber threats into clear business insights. Rather than concentrating on technical security operations, the course emphasizes analytical thinking, governance awareness, and structured evaluation of cybersecurity risks in relation to organizational objectives.

Throughout the program, participants strengthen analytical thinking for cybersecurity analysts, enhance their ability to evaluate cybersecurity governance and controls, and apply business-driven cyber risk assessment approaches. The course enables professionals to contribute confidently to cybersecurity decision support analysis, improve stakeholder communication in cybersecurity, and align cybersecurity considerations with enterprise priorities.

Target Audience

- Business Analysts
- Senior Business Analysts
- Cybersecurity Analysts with a business focus
- Risk Management Professionals
- Governance and Compliance Specialists
- Digital Transformation Managers
- Strategy and Planning Professionals
- IT–Business Interface Roles

AGILE LEADERS
Training Center

Targeted Organizational Departments

- Business Analysis & Enterprise Architecture
- Risk Management & Enterprise Risk
- Cybersecurity Governance & Oversight
- IT Strategy & Digital Transformation
- Compliance, Audit & Internal Control
- Operations & Business Continuity
- Corporate Strategy & Planning

Targeted Industries

- Government & Public Sector
- Banking, Financial Services & Insurance
- Healthcare & Life Sciences
- Energy, Utilities & Oil & Gas
- Telecommunications
- Transportation & Critical Infrastructure
- Large Enterprises in Regulated Sectors

Course Offerings

By the end of this course, participants will be able to:

- Apply cybersecurity analysis competencies within enterprise environments
- Perform cyber risk identification and analysis using structured analytical techniques
- Conduct business impact analysis for cybersecurity incidents and scenarios
- Evaluate cybersecurity governance and controls from a business perspective
- Support leadership through cybersecurity decision support analysis
- Communicate cyber risks effectively to business and executive stakeholders
- Apply risk-based cybersecurity analysis to support strategic decisions
- Define and execute the business analyst role in cybersecurity initiatives
- Perform requirements and controls analysis in cybersecurity contexts

Training Methodology

The Certificate in Cybersecurity Analysis IIBA-CCA applies an interactive, competency-driven training methodology tailored for experienced professionals. Learning is delivered through facilitated discussions, guided analysis sessions, structured group activities, and scenario-based exercises reflecting real organizational cybersecurity challenges.

Participants actively practice business-focused cybersecurity analysis by examining risk, impact, and governance situations commonly faced in enterprise environments. Emphasis is placed on analytical reasoning, decision support, and stakeholder communication rather than technical security execution. Daily reflection sessions reinforce learning and enable participants to connect cybersecurity analysis activities to organizational strategy, governance, and performance objectives.

Course Toolbox

- Cybersecurity analysis frameworks illustrative examples
- Business-driven cyber risk assessment scenarios
- Business impact analysis walkthroughs
- Governance and control evaluation examples
- Stakeholder communication and reporting illustrations
- Cybersecurity decision support case discussions

AGILE LEADERS
Training Center

Course Agenda

Day 1: Foundations of Cybersecurity Analysis for Business

- **Topic 1:** Cybersecurity analysis competencies and professional expectations
- **Topic 2:** Business analysis in cybersecurity environments
- **Topic 3:** Cybersecurity analysis capability framework
- **Topic 4:** Cyber risk concepts for business analysts
- **Topic 5:** Analytical thinking for cybersecurity analysts
- **Topic 6:** Enterprise context and value-driven cybersecurity analysis
- **Reflection & Review:** Core principles of business-focused cybersecurity analysis

Day 2: Cyber Risk Identification and Assessment

- **Topic 1:** Cyber risk identification and analysis techniques
- **Topic 2:** Business-driven cyber risk assessment approaches
- **Topic 3:** Threats, vulnerabilities, and business exposure
- **Topic 4:** Risk prioritization using analytical criteria
- **Topic 5:** Cybersecurity risk analysis training scenarios
- **Topic 6:** Translating cyber risks into business language
- **Reflection & Review:** Applying risk-based cybersecurity analysis

Day 3: Business Impact and Requirements Analysis

- **Topic 1:** Business impact analysis for cybersecurity events
- **Topic 2:** Operational, financial, and reputational impact evaluation
- **Topic 3:** Requirements and controls analysis in cybersecurity
- **Topic 4:** Aligning cybersecurity requirements with business objectives
- **Topic 5:** Value-focused prioritization of cybersecurity initiatives
- **Topic 6:** Managing dependencies and constraints
- **Reflection & Review:** Linking cybersecurity impact to enterprise value

AGILE LEADERS
Training Center

Day 4: Governance, Controls, and Stakeholder Communication

- **Topic 1:** Cybersecurity governance and controls overview
- **Topic 2:** Evaluating control effectiveness from a business perspective
- **Topic 3:** Governance structures, roles, and accountability
- **Topic 4:** Stakeholder communication in cybersecurity initiatives
- **Topic 5:** Executive and leadership cyber risk reporting
- **Topic 6:** Managing trade-offs in cybersecurity decisions
- **Reflection & Review:** Strengthening governance and communication

Day 5: Decision Support and Strategic Cybersecurity Analysis

- **Topic 1:** Cybersecurity decision support analysis frameworks
- **Topic 2:** Supporting investment and prioritization decisions
- **Topic 3:** Professional responsibilities in cybersecurity analysis
- **Topic 4:** Integrating cybersecurity analysis into enterprise strategy
- **Topic 5:** The business analyst role in cybersecurity leadership
- **Topic 6:** Sustaining cybersecurity analysis capability
- **Reflection & Review:** Embedding cybersecurity analysis in practice

FAQ

What specific qualifications or prerequisites are needed for participants before enrolling in the course?

Participants should have prior experience in business analysis, risk management, governance, or enterprise decision-making roles. A technical cybersecurity background is not required.

How long is each day's session, and is there a total number of hours required for the entire course?

Each day's session is generally structured to last around 4–5 hours, with breaks and interactive activities included. The total course duration spans one week, approximately 20–25 hours of instruction.

Is this course technical or focused on cybersecurity operations?

No. This course is strictly focused on cybersecurity analysis from a business perspective, emphasizing risk analysis, impact assessment, governance, and decision support.

AGILE LEADERS
Training Center

How This Course Is Different from Other Certificate in Cybersecurity Analysis IIBA-CCA Courses

This course is designed as a pure competency-development program, not a technical cybersecurity or exam-preparation course. It emphasizes business-focused cybersecurity analysis, enabling participants to apply analytical thinking, governance insight, and structured decision support within real organizational contexts.

Unlike generic cybersecurity training, the program strengthens cyber risk analysis for business analysts, business impact analysis for cybersecurity, and stakeholder communication in cybersecurity, ensuring direct applicability to leadership decision-making and enterprise risk governance.