

OUR LEARNING EXCLUSIVE

- Custom exam prep software and materials
- Course-specific thinQtank® Learning publications to make the learning fun and engaging
- Scenario workshops and practice questions every day
- We do not teach the test. We always deliver valuable hands-on experience
- All reading material and study guides sent to you when you register
- Every course taught by experienced ISACA-certified practitioners
- Six months mentoring access to our engineers after the course

TRAINING CAMP FORMAT

thinQtank® Learning delivers this course as a **five-day instructor-led training camp, Monday to Friday**. About 60% lecture and 40% hands-on labs and practice exams. Hands-on work is set to suit the group and the delivery method. Contact us for the schedule covering your dates.

PREREQUISITES

- No formal prerequisite
- ISACA recommends 2-3 years of cybersecurity experience

TARGET AUDIENCE

- SOC analysts (Tier 1 and 2)
- Junior incident responders
- IT and network staff moving into cyber operations
- DoD and government cyber defense personnel
- Service members, veterans and military spouses using AF COOL, Army CA, MyCAA or VET TEC 2.0

EXAM

Exam	ISACA Certified Cybersecurity Operations Analyst (CCOA)
Exam fee	\$499 USD per attempt, set by ISACA
Format	140 questions in 240 minutes: 115 multiple-choice and 25 performance-based questions using open-source tools
Passing	Not published by ISACA
Delivery	Testing center or online proctored; we help you schedule

DELIVERY METHODS

- Instructor-led training
- Immersive live-online training
- On-site and custom delivery

COURSE OVERVIEW

thinQtank® Learning is offering a unique five-day training camp comprised of five days of instructor-led learning that gives students the knowledge and skills needed to work in cybersecurity operations: technology essentials, cybersecurity principles and risk, adversary tactics and MITRE ATT&CK, incident detection and response with SIEM and EDR, and securing assets.

CCOA is ISACA's hands-on certification for SOC and cyber operations analysts, with performance-based questions on real open-source tools.

This course prepares you for the **ISACA Certified Cybersecurity Operations Analyst (CCOA)** exam.

WHAT YOU WILL BE ABLE TO DO

- Work confidently with networks, endpoints, cloud apps, APIs and scripts
- Apply security principles and assess application, cloud and supply-chain risk
- Map attacks to MITRE ATT&CK
- Detect and investigate with logs, SIEM, EDR and indicators of compromise
- Handle incidents, including forensics, malware and packet analysis
- Secure assets with IAM, hardening and vulnerability management

COURSE OBJECTIVES

Primary course objectives, following the official exam outline:

- Incident Detection and Response
- Technology Essentials
- Cybersecurity Principles and Risk
- Securing Assets
- Adversarial Tactics, Techniques and Procedures

EXCLUSIVE LEARNING PACKAGE

- thinQtank® Learning Accelerated Custom Exam Study Guide for this exam
- Practice exams built to the official exam outline
- Additional hours of remote lab access
- Custom video recordings for review
- Retake any or all of the course, in person or live online, for 24 months

ISACA CERTIFICATION PATH

CCOA

Cybersecurity operations

CISM

Security management

AAISM

AI security management

COURSE MODULES

01 Incident Detection and Response

34% of exam

- › Topic A: Logs, SIEM, EDR and indicators of compromise
- › Topic B: Incident handling
- › Topic C: Forensics, malware and packet analysis

02 Technology Essentials

25% of exam

- › Topic A: Networking
- › Topic B: Systems and endpoints
- › Topic C: Cloud, APIs and scripting

03 Cybersecurity Principles and Risk

20% of exam

- › Topic A: Security principles and governance
- › Topic B: Application, cloud, data and supply-chain risk

04 Securing Assets

11% of exam

- › Topic A: Identity and access management
- › Topic B: Hardening
- › Topic C: Vulnerability management and contingency planning

05 Adversarial Tactics, Techniques and Procedures

10% of exam

- › Topic A: Threat landscape
- › Topic B: Attack stages and exploit techniques
- › Topic C: MITRE ATT&CK

TERMS

© 2026 thinQtank® Global, Inc. All rights reserved. This course datasheet and the course materials it describes are protected by U.S. and international copyright laws. thinQtank Global and thinQtank Learning are registered trademarks of thinQtank Global, Inc. ISACA, CGEIT, CDPSE, CCOA, AAIR, CISA, CISM and CRISC are trademarks of ISACA. All other names and marks are the property of their respective owners. thinQtank Learning is an independent training provider and is not affiliated with or endorsed by ISACA unless stated.

Course content, exam outlines and vendor exam fees are subject to change by the certification vendor. Exam weights shown are taken from the vendor's published exam guide at the time of printing.

THE COURSE AND LEARNING MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. THINQTANK GLOBAL, INC. SHALL NOT BE LIABLE FOR ANY INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING FROM THE USE OF THE COURSE OR LEARNING MATERIALS, AND DOES NOT GUARANTEE THAT A STUDENT WILL PASS ANY CERTIFICATION EXAM.

The learning materials are licensed for the student's own internal understanding and operation of the technology covered, and may not be copied, redistributed or used to deliver training without written permission from thinQtank Global, Inc.