

C|CISO TRAINING

CERTIFIED CHIEF INFORMATION SECURITY OFFICER

DATE:
18 - 21 September
PRAGUE

The C|CISO certification is an industry-leading program that recognizes the real-world experience necessary to succeed at the highest executive levels of information security. Bringing together all the components required for a C-Level positions, the C|CISO program combines audit management, governance, IS controls, human capital management, strategic program development, and the financial expertise vital for leading a highly successful IS program.

The C|CISO Training Program can be the key to a successful transition to the highest ranks of information security management.

POWERED BY:

QuBit
Conference

EC-Council

KEY TAKE-AWAY:

- Establishes the role of CISO and models for governance
- Core concepts of information security controls, risk management, and compliance
- Builds foundation for leadership through strategic planning, program management, and vendor management

THE TRAINER:



Tom Brett is a business training expert with 25+ years' experience in the field of IT and Cyber security. Working for the IPA in Ireland, he has delivered training briefings across all levels of an organisation from Directors to Senior Managers and Staff.

Top 3 reasons you should consider attaining the Certified CISO Certification

1. C|CISO WAS DESIGNED BY CISOs
2. C|CISO IS NOT FOCUSED ON THE TECHNICAL ASPECTS OF THE CISO JOB ROLE
3. C|CISO COVERS STRATEGIC AND FINANCIAL MANAGEMENT

5 Domains of the Training:

- Governance
- Security risk management, controls, and audit management
- Security program management and operations
- Information security core concepts
- Strategic planning, finance, and vendor management

CONTACT US

For more information on our C|CISO Training, please contact our Sales Department at:
tatiana@qubitacademy.com

C|CISO TRAINING

CERTIFIED CHIEF INFORMATION SECURITY OFFICER

DATE:
18 - 21 September
PRAGUE

TRAINING SCHEDULE

DAY 1: Domain 1 –Governance

C|CISO Book of Knowledge (BOK) has; 4 Chapters, 76 Pages, 241 –Class Slides

Morning

Introduction–Meet and Greet (Know all and gauge expectations)

1stPresentation –All 5–Days Program

2ndPresentation –Cybersecurity in New Era

3rdPresentation –Information Security (Overview)

4thPresentation –C|CISO Domain 1 –Governance

Afternoon

C|CISO Domain 1 –Governance (Continuance)

Team Exercise:

(a) Build Governance, Risk & Compliance Framework Structure

(b) Create for Group Security Office –Information Access Management Policy

DAY 3: Domain 3 - Security Program Management and Operations

C|CISO Book of Knowledge (BOK) has; 4 Chapters, 39 Pages, 172 –Class Slides

Morning

Takeaways from Participants understanding

1stPresentation

C|CISODomain 3 –Security Program Management and Operations

Afternoon

C|CISO Domain 3 –SPM and Operations (Continuance)

Team Exercise:

(a) Build for GSO, Group Information Security Portfolio,Project and Program Management (Excel Template)

(b) Createand Manage the GSO –Section wise Work stream Tracker for Higher Management reporting

DAY 2: Domain 2–Security Risk Management, Controls and Audit Management

C|CISO Book of Knowledge (BOK) has; 5 Chapters, 37 Pages, 174 –Class Slides

Morning

Takeaways from Participants understanding
1stPresentation

C|CISODomain 2 –Security Risk Management, Controls and Audit Mngmt.

Afternoon

C|CISO Domain 2 –SRM, Controls and AM(Continuance)

Team Exercise:

(a) Mapping of MAS and ISO27001:2013 Controls to the IAM Policy

(b) How IAM Policyis Implemented in your Organization

(c)How Internal / External Auditorsshall Audit it? Adequacy and Effectiveness

(d) Discuss MAS–TRM Framework

DAY 4: Domain 4 –Information Security Core Competencies

C|CISO Book of Knowledge (BOK) has; 6 Chapters, 47 Pages, 198 –Class Slides

Morning

1stPresentation –C|CISODomain 4 –Information Security Core Competencies

Domain 5 –Strategic Planning, Financial Management and Vendor Management

C|CISO Book of Knowledge (BOK) has; 3 Chapters, 24 Pages, 108 –Class Slides

Afternoon

2ndPresentation –C|CISO Domain 5 –Strategic Planning, Financial Management and Vendor Management

Team Exercise

(a) Buildingof Group Information Security Strategy and Objectives

(b) Build Group Information Security SteeringCommittee Charter (ISSCC)