PREPARATION COURSE TO THE CERTIFIED INFORMATION SECURITY MANAGER® (CISM®) CERTIFICATION

ONLINE PROGRAMME - 7, 9, 14 & 16 NOVEMBER 2022

ORGANISATION SHEET

Objective

The primary objective of this course is to enable participants to get ready to take the CISM® exam.

Methodology

This interactive course is an ideal way to prepare for the CISM® exam.

The preparation courses focus exclusively on the essential areas covered in the CISM® certification exam. The course covers the core sections and a series of sample exam questions that provides participants with a “feel” of the format and the types of questions encountered during the exam. The correct answers to each question are also reviewed for a better understanding of expectations of the ISACA Certification Board.

Selected participants will receive the CISM® material in advance to study before taking part in the course. Please note that the CISM® exam requires long-term preparation and self-study.

Target Audience

Information Security Managers, Chief Information Officers, Risk Managers from commercial banks, central banks and supervision authorities or other financial institutions

- willing to take the CISM® exam, for which they must have
- a **minimum of 5 years** of information security management work experience within the past 10 years in order to qualify for the CISM® certification.

  Experience must be earned in three of the four CISM® Job Practice Domains to qualify:
  - Information Security Governance
  - Managing Information Risk Management
  - Information Security Program
  - Incident Management

Examination

Following this training programme, candidates are requested to take the CISM® exam **by the 31 December 2022**.

The exam can be taken in a remote proctoring format or in person at a test centre (available in most of our partner countries - please refer to the CISM® Exam Information document to check if there is a center in your country).

Trainer

Mr Germain Geissler

Germain works at RBC Investor & Treasury Services Luxembourg as Associate Director in charge of Cyber and Technology Risk. He is responsible for having independent oversight of the information security systems and related operational functions, controls, and processes.

Germain Joined RBC in April 2018 and has previously worked for various companies such as Deloitte and Clearstream, on various cyber security engagements covering a broad range of areas such as Business Continuity Management, Digital Forensic, Internal Control.

Germain has also been an Accredited Trainer for ISACA Luxembourg Chapter since 2017. He has been an instructor for multiple CISA, CISM and CRISC trainings provided to participants such as Big 4 Audit and Advisory teams.

Germain holds various certifications such as the CISA, CISM, CRISC, CISSP, and ISO 22301 Lead Auditor / Lead Implementer.

Language

English

Dates & Time

4 sessions of 4hours
7, 9, 14 & 16 November 2022 from 8.30 to 12.30 CET

Platform & Technical requirements

Webex

In order to join the course participants are requested to have:

- a stable internet connection
- a device (preferably a PC) with well-functioning microphone and webcam, which is mandatory to be able to interact with the trainer and their peers.

PREPARATION COURSE TO THE CERTIFIED INFORMATION SECURITY MANAGER® (CISM®) CERTIFICATION

ONLINE PROGRAMME - 7, 9, 14 & 16 NOVEMBER 2022

CONTENT

Program:
The ISACA CISM® Exam Preparation Training covers the following 4 job practice domains:

Domain 1 - Information Security Governance (17%)
Affirms the expertise to establish and/or maintain an information security governance framework (and supporting processes) to ensure that the information security strategy is aligned with organizational goals and objectives. Domain 1 confirms your ability to develop and oversee an information security governance framework to guide activities that support the information security strategy.

Domain 2 - Managing Information Risk Management (20%)
Proficiency in this key realm denotes advanced ability to manage information risk to an acceptable level, in accordance with organizational risk appetite, while facilitating the attainment of organizational goals and objectives. Domain 2 demonstrates expertise in classifying information assets to ensure measures taken to protect those assets are proportional to their business value.

Domain 3 - Information Security Program (33%)
Establishes ability to develop and maintain an information security program that identifies, manages and protects the organization’s assets while aligning with business goals. Domain 3 attests to the ability to ensure the information security program adds value while supporting operational objectives of other business functions (human resources, accounting, procurement, IT, etc.).

Domain 4 - Incident Management (30%)
Validates capacity to plan, establish and manage detection, investigation, response and recovery from information security incidents in order to minimize business impact. Domain 4 establishes your skills in accurately classifying and categorizing information security incidents and developing plans to ensure timely and effective response.

Remark: By delivery date, any training documentation shall be subject to regular reviews and updates amending the table of content as described herein.

This training is provided with the support of THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG