Auditing the Cybersecurity Program Certificate

Product Details

Internal audit should play a key role in supporting the organisation in reducing cyber risk. Cybersecurity program auditing can serve as the critical barrier between a potential cyber-attack and the organisation. Due to the cost, risk, an repetitional damage that can result from a cyber incident or data breach, every organisation needs a cyber strategy and response plan.

Participants who complete the course are eligible to sit for the certificate exam which is administered on the IIA's LMS platform.

Each course segment concludes with a short multiple-choice quiz, requiring an 80% score to pass. Participants can retake these quizzes as often as needed to achieve mastery. After completing all segments, participants must pass a 40 multiple-choice certificate exam. The exam allows up to three attempts before a retake fee is required.

LEARNING OBJECTIVES

- Recognize what drives cyber risk and how internal audit can assess control effectiveness
- Identify how to assess data storage solutions
- Define digital transformation, digitalization risks, and associated controls
- Recognize characteristics of a typical, timely patch management process
- Explain key concepts relating to the vulnerability management program, including commonly applied vulnerability management maturity models
- Identify how automation of business impacts the methods used in audit testing
- Investigate méthodes to reduce risk exposure from common API and web services vulnerabilities
- Determine how to mitigate risk exposure from common privileged access management vulnerabilities
- Identify methods to adjust audit approches for DevSecOps
- Review how to mitigate risk exposure from common SoD vulnerabilities in DevSecOps Applications
- Understand internal audit's role in continuous monitoring and continuous auditing
- Recall objectives and methods deployed in red team exercises
- Recall important factors relating Security Operations Centers (SOC) and incident management, monitoring, detection, and response frameworks
- Identify controls, and associated assessments, needed to operate a SOC

WHO WILL BENEFIT?

- This certificate program is designed to ensure the internal audit community processes the fundamental competencies to effectively assess an organisation's cybersecurity governance and management practices, including their cybersecurity program capabilities. This program is intended for operational internal auditors and audit leaders who want to deepen their understanding and gain recognition of their cybersecurity knowledge.
- Participants who successfully complete this program are eligible to plus themselves by obtaining The Auditing the Cybersecurity Program Certificate - a wonderful addition to both your resume and LinkedIn profile.

Course Information

- Course duration : **2,5** days (5*4 hours)
- Participants who complete the course are eligible to sit for the certificate exam which is administered on The IIA's LMS platform.
- CPE Hours available : 20
- Competency level : Applied knowledge
- Prerequisites : Fundamentals of Cybersecurity or equivalent knowledge
- Exam : 40 questions

PRICE & SESSIONS

- **1900€** ex VAT for members (2400€ ex VAT for non-members)
- **2025 (5*9h-13h CET - by Zoom)** :
  - June 2nd to 6th
  - Sept 29th to Oct. 3rd
  - Nov. 17th to 21st

Course content

1. **Auditing the Cybersecurity Program :**
   - Importance of the cybersecurity Program
   - Drivers of cybersecurity risk
   - Manage cybersecurity risk
   - The cybersecurity program audit plan

2. **Auditing Storage Management Solution and Containers :**
   - Overview of storage management solutions and containers
   - Data storage compliance landscape
   - Auditing ephemeral and micro-services
   - Cloud provider data storage tools and their benefits
   - Adopting continuous auditing for data protection, retention, and destruction

3. **Auditing Digital Transformation and Digitization Programs :**
   - Key concepts of digital transformation and digitization
   - Digital technologies and risks
   - Internal audit's role in digital initiatives
   - Auditing digitization programs
   - Auditing digital transformation programs

4. **Auditing the Vulnerability Management Program**
   - Vulnerability management program overview
   - Understand common vulnerability management maturity models used to assess organizational cybersecurity vulnerabilities
   - Review key metrics for auditing the vulnerability program
   - How to implement appropriate actions when auditing vulnerabilities

5. **Auditing the Patch Management Program**
   - Key concepts of patch management
   - Understand typical, timely patch management process
   - How the patch management program reduces cybersecurity risk and organizational vulnerabilities
   - How the patch management program reduces data breach risk and loss

6. **Auditing automation**
   - Automation impact on audit testing
   - Effective audit automation
   - Visualize the risks of automation when establishing the internal audit scope
   - Auditing automation

7. **Auditing API and Web Services**
   - API and web services overview
   - Audit and test API and web services security
   - Reduce API-bases web services risk

8. **Auditing privileged Access Management**
   - Key concepts of privileged access management
   - Types and purposes of privileged access management
   - Inventory and audit privileged access management
   - Mitigate risk exposure from common privileged access management cyberattacks

9. **Auditing DevSecOps**
   - DevSecOps overview
   - The DevSecOps development process
   - Issues and controls
   - Auditing DevSecOps

10. **Auditing Continuous Monitoring**
    - Auditing continuous monitoring process components
    - Internal audit's role in incorporating data analytics and continuous monitoring into the organization
    - Develop a simplified yet high-impact reporting mechanism to meet a variety of stakeholders needs
    - Continuous monitoring, high impact reporting, agile audit approach and dynamic risk assessment methodologies

11. **Auditing Red, Blue, and Purple Team Testing**
    - Overview of the kill chain and types of attacks
    - Points of vulnerability as it relates to people, technologies and systems
    - Identify areas of improvement in defensive incident response processes across every phase of the kill chain
    - Establish the organization's first-hand experience to detect and contain a targeted attack

12. **Auditing the Security Operations Center (SOC)**
    - Key concepts of the SOC
    - SOC processes and checklists
    - Controls needed to operate a SOC