The Institute of Internal Auditors Greece

Auditing the Cybersecurity Program Certificate

Zois Sompolos

About This Instructor-Led Certificate Program

With cyber-attacks growing at alarming rates around the globe, and data breaches increasing by 37 percent in just on quarter (according to Statista) at a staggering average cost of $4.24 million USD (according to IBM), it is no wonder law makers are focusing on cyber-focused regulations.

International laws including EU's GDPR, German IT Security Law, and US Principles for Cyber Incident Reporting, and US Global Cyber Incident Reporting Policy Principles are a few examples where governments world-wide are articulating the need for strong cyber controls and increased transparency regarding cyber-related incidents. Additional proposals are under consideration by governments around the world including the proposed SEC cyber reporting rules. With the increased scrutiny, it is in the strategic best interest of both public and private organizations to audit their cybersecurity programs.

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

Course Objectives

- Recognize what drives cyber risk and how internal audit can assess control effectiveness.
- Identify how to assess data storage solutions.
- Define digital transformation, digitization 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 processes impacts the methods used in audit testing.
- Investigate methods 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 approaches 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 to Security Operations Centers (SOC) and incident management, monitoring, detection, and response frameworks.
- Identify controls, and associated assessments, needed to operate a Security Operations Center (SOC).

Who should attend?

This certificate program is designed to ensure the internal audit community possesses the fundamental competencies to effectively assess an organization'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 IIA ESG Certificate- a wonderful addition to both your resume and LinkedIn profile.

Auditing the Cybersecurity Program Certificate

Price
€ 2300
€ 1220 (members IIA Greece)

Venue
virtual seminar via tele-conference

CPE's: 21

ΩΡΕΣ: 24

Καλύπτει τις απαιτήσεις του Ν.4849/2024 για τους Εσωτερικούς Ελεγκτές

Certificate Topics

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

Auditing Storage Management Solutions 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.

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.

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.

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.

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

Auditing API and Web Services
- API and web services overview.
- Audit and test API and web services security.
- Reduce API-based web services risk.

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.

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

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 stakeholder needs.
- Continuous monitoring, high impact reporting, agile audit approach and dynamic risk assessment methodologies.

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.

Auditing the Security Operations Center
- Key concepts of the Security Operations Center (SOC).
- Security Operations Center (SOC) processes and checklists.
- Security Operations Center (SOC) Framework for incident management, monitoring, detection, and response.
- Controls needed to operate a Security Operation Center (SOC).

Βιογραφικό Εισηγητή

Mr. **Zois P. Sompolos** is an experienced Internal Auditor with over 12 years of expertise in Internal Audit, particularly focusing on Information Systems. His professional journey began with significant academic involvement, participating in various research and teaching projects at the University of Patras, Greece, from 2001 to 2005. In 2006, he joined the National Bank of Greece Group and in 2012, he was selected to join the Group Internal Audit Department, where he currently holds the role of Audit Manager. Additionally, he has been serving as an educator for the Institute of Internal Auditors since 2022.

Mr. Sompolos's educational background is extensive and diverse. He holds a BSc and PhD in Physics and an MSc in Environmental Sciences from the University of Patras, as well as a BSc in Computer Science and an MBA in Business Administration from the Hellenic Open University. Further enhancing his expertise, he completed a specialization in Artificial Intelligence and Machine Learning for Financial Services at the National and Kapodistrian University of Athens in 2020.

Certified in various professional domains, Mr. Sompolos is a Certified Internal Auditor (CIA), Certified Information Systems Auditor (CISA), and holds multiple other certifications, including Analytics Certified Data Analyst (ACDA), IT General Controls (ITGC), Auditing the Cybersecurity Program (ACP), and Data Analytics and Literacy (DAL).

His main interests lie in the security and control of information systems, data analysis, data visualization, and the application of advanced techniques such as machine learning, benchmarking, and outlier detection to extract valuable insights from data.

The Institute of Internal Auditors Greece

Registration - Information: tel. +30 210 8259504, e-mail: training@hiia.gr