



PB INSTITUTE OF RESEARCH AND TECHNOLOGY

P.O Box 21457-00100

Nairobi - Kenya

Mobile: +254 721 214 795

Email: info@pebblesinstitute.org

Cybersecurity Risk Quantification For Auditors Training

Duration: 5 days

On-Site

01 Who Should Attend

- This course is ideal for;
- Internal Auditors
- IT Auditors
- Financial Auditors
- Risk Management Professionals
- Information Security Leaders (CISOs, CIOs)
- Compliance Officers
- Actuaries & Quantitative Analysts
- Governance, Risk, and Compliance (GRC) Specialists

02 About the Course

In today's interconnected digital landscape, cybersecurity risk quantification has emerged as a crucial discipline, empowering auditors to move beyond qualitative assessments and truly understand the financial impact of cyber threats on an organization's bottom line. This essential training course focuses on Cybersecurity Risk Quantification for Auditors, equipping participants with the specialized knowledge and practical methodologies to measure cyber risks in monetary terms, enabling more informed decision-making and strategic resource allocation. You will learn to apply quantitative models to assess potential losses from cyber incidents, prioritize security investments based on demonstrable financial benefit, and communicate complex cyber risks in a language that resonates with executive leadership and boards.



PB INSTITUTE OF RESEARCH AND TECHNOLOGY

P.O Box 21457-00100

Nairobi - Kenya

Mobile: +254 721 214 795

Email: info@pebblesinstitute.org

03 Workshop Objectives

- ??? Understand the fundamental concepts of cybersecurity risk quantification (CRQ).
- Learn the limitations of qualitative risk assessment and the benefits of a quantitative approach.
- Master various methodologies and frameworks for cybersecurity risk quantification.
- Develop skills in identifying relevant data and metrics for CRQ analysis.
- ??? Understand how to apply statistical models (e.g., Monte Carlo simulations) to cyber risk.
- Learn about estimating potential financial losses from various cyber scenarios.
- Explore best practices for communicating quantified cyber risks to executive stakeholders.
- Master techniques for prioritizing cybersecurity investments based on ROI.
- Understand the integration of CRQ into the overall audit process.
- Learn about tools and technologies supporting cybersecurity risk quantification.
- Apply practical CRQ techniques to real-world cybersecurity audit scenarios.

04 Module Topics

Module 1: Introduction to Cybersecurity Risk Quantification

- Defining cybersecurity risk quantification (CRQ) and its strategic importance for auditors.
- Understanding the limitations of traditional qualitative risk assessments.
- Exploring the benefits of measuring cyber risk in financial terms.
- Overview of key concepts: ARO, SLE, ALE, and Monte Carlo simulation.
- Setting the stage for a data-driven approach to cybersecurity auditing.

Module 2: Methodologies & Frameworks for CRQ



PB INSTITUTE OF RESEARCH AND TECHNOLOGY

P.O Box 21457-00100

Nairobi - Kenya

Mobile: +254 721 214 795

Email: info@pebblesinstitute.org

- Learning various CRQ methodologies (e.g., FAIR, OpenFAIR) and their underlying principles for your module.
- Understanding the stages of a quantitative risk assessment.
- Exploring different frameworks for categorizing and modeling cyber threats.
- Comparing and contrasting various CRQ approaches.
- Selecting the appropriate methodology for an audit context.

Module 3: Data Collection and Metrics for CRQ

- Identifying and sourcing relevant data for cybersecurity risk quantification for your module.
- Understanding metrics related to asset values, threat event frequencies, and control effectiveness.
- Learning about data normalization and cleansing for CRQ input.
- Utilizing internal security data, industry benchmarks, and threat intelligence.
- Addressing data gaps and assumptions in CRQ analysis.

Module 4: Applying Statistical Models to Cyber Risk

- Introduction to statistical models used in cybersecurity risk quantification for your module.
- Mastering the use of Monte Carlo simulations to model financial losses from cyber events.
- Understanding probability distributions (e.g., Normal, Log-Normal, PERT) in CRQ.
- Interpreting simulation results and confidence intervals.
- Hands-on exercises with CRQ modeling tools.

Module 5: Estimating Financial Losses from Cyber Incidents

- Techniques for estimating various components of financial losses from cyber incidents for your module.
- Quantifying direct costs (e.g., breach response, fines, legal fees).
- Assessing indirect costs (e.g., reputational damage, customer churn, business interruption).
- Developing loss event scenarios and their associated financial impacts.
- Applying structured estimation techniques (e.g., calibrated estimation).



PB INSTITUTE OF RESEARCH AND TECHNOLOGY

P.O Box 21457-00100

Nairobi - Kenya

Mobile: +254 721 214 795

Email: info@pebblesinstitute.org

Module 6: Communicating Quantified Cyber Risks

- ▶ Strategies for effectively communicating quantified cyber risks to diverse stakeholders for your module.
- ▶ Presenting financial risk scenarios to executive leadership and boards.
- ▶ Tailoring reports to resonate with financial, operational, and technical audiences.
- ▶ Visualizing risk exposure and potential loss distributions clearly.
- ▶ Translating complex quantitative results into actionable insights.

Module 7: CRQ Integration in the Audit Process

- ▶ Integrating cybersecurity risk quantification into the internal and external audit process for your module.
- ▶ Using CRQ results to prioritize audit scope and focus.
- ▶ Evaluating the effectiveness of controls based on their financial impact on risk reduction.
- ▶ Providing assurance on the accuracy and reliability of cyber risk quantification models.
- ▶ Leveraging CRQ to drive more strategic and impactful cybersecurity audits