CYBER RISK QUANTIFICATION WORKSHOP

Measuring, Quantifying and Communicating Your Cybersecurity Posture

16 - 20 March, 2020

Gaborone, Botswana

Eligible and Certified ISACA Participants Will Earn CPE Hours

Organised and Facilitated by;

African Cyber Security Botswana

SERIANU

Workshop Overview

P8,000
Cost Per Delegate
exclusive of taxes

50+
Attendees

5
Days

7
Countries

16
Sessions

Course Summary

Are you struggling to measure and communicate your current cybersecurity risk posture in monetary terms? This workshop will enable ICT, Audit, Operations and Risk Management professionals to provide ExCo, the Board and regulators with objective, quantifiable and observable cyber security metrics to enable key stakeholders to make strategic decisions.

Serianu Limited is pleased to invite you to a 5-day workshop that will guide you on measuring and quantifying cybersecurity risks.

Objectives

- Understand how to define, develop, maintain and communicate an effective risk profile and appetite statement to ExCo and Board members.
- Discuss new holistic, risk-based, business-driven approach to measure, benchmark and track maturity of your cybersecurity program.
- Understand how to develop cyber risk metrics that are quantifiable, observable, and objective data supporting metrics. This will involve the use of metrics to facilitate decision making and improve performance and accountability.
- Discuss how to determine an organization's cyber risk tolerance level using the organizations current risk investments and potential exposure or losses.

Target Audience

- ICT and Information Security Professionals
- Risk Management and Audit Officers
- Legal and Compliance Officers
- Finance and Strategy Managers

Course Schedule

	DAY ONE	DAY TWO	DAY THREE	DAY FOUR	DAY FIVE
	CYBERSECURITY TRENDS, RISK PROFILING AND APPETITE	**CYBERSECURITY BENCHMARKING AND MATURITY ASSESSMENTS**	**VISIBILITY AND RESILIENCE MONITORING AND REPORTING**	**RISK TOLERANCE AND PRIORITIZATION**	**EXCURSION**
8:30 - 10:30					
	Emerging Trends and Top Priorities for African Organizations	Benchmarking using CVEQ	Visibility and Resilience controls	Risk Tolerance Analysis	
11:00 - 1:00					
	Inherent Risk Profiling	Maturity Assessment using CVEQ	CVEQ Exposure Analysis	Risk Prioritization	
	LUNCH TIME				
2:00 -3:00					
	Risk Exposure Analysis	Meeting Compliance needs using CVEQ	Incident Monitoring and Analysis	Reporting to the Board and ExCo	
3:00 - 4:00					
	Case Study	Case Study	Case Study	Case Study	
	End of Class				

Course Topics In Detail

DAY 1

Risk Profiling and Appetite

Participants will be taken through the process of measuring risk exposure resulting from an organization's activities, services and products. It will also involve understanding of an organization's risk appetite through establishing a baseline of exposures and tolerances defined by senior management.

DAY 2

Program Maturity and Benchmarking

Participants will be taken through how to establish the current state of business processes and performance metrics with the aim of developing a roadmap of key milestones needed for optimizing the cybersecurity posture within an organization.

DAY 3

Visibility and Exposure

Participants will be taken through the process of measuring the effectiveness and efficiency of implemented technical and process cybersecurity controls within an organization. The goal of this is to be able to deliver an unobstructed view into the operation of security controls within a network environment therefore making it easier to manage.

DAY 4

Risk Tolerance and Prioritization

Participants will be taken through the process of adequately determining the maximum negative impact (loss amount) that senior management should be willing to accept from a specific risk event or series of risk events. The tolerance levels will be derived from exposure quantification.

Course Breakdown

Lesson 1 — Cybersecurity Trends, Risk Profiling and Appetite

Introduction
- Emerging Trends
- Threat Actors and their Motives
- Top Risks
- Cause and Effect Matrix
- Top Priorities for African Organizations

Cyber Risk Profiling
- The Inherent Risk Profile
- Categories of the Inherent Risk Profile
- Measuring the Risk
- Measuring Overall Inherent Risk Profile

Cyber Risk Exposure Analysis
- Governance and Processes around Cyber Risk Appetite
- Preparing, Reviewing and Reporting the Cyber Risk Appetite Statement
- Risk Appetite Framework Metrics

Introduction to Cyber Visibility and Exposure Quantification (CVEQ)

Lesson 2 — Cybersecurity Benchmarking and Maturity Assessments

Introduction
- Cybersecurity Frameworks
- Cyber Visibility & Exposure Quantification (CVEQ)
- Benchmarking using CVEQ
- Weighted Score
- Maturity Assessment using CVEQ
- Calculating Cybersecurity Maturity
- Meeting compliance needs with CVEQ Framework
  - Domain 1: Cybersecurity Risk Management
  - Domain 2: Cybersecurity Asset Management
  - Domain 3: Cyber User Management
  - Domain 4: Cyber Incident Management
  - Domain 5: Cyber Continuity Management

Lesson 3 — Visibility and Exposure Analysis

Introduction
- Visibility Controls
- Testing of Controls – Existence, Completeness, Timeliness, Reporting

Exposure Analysis

Lesson 4 — Monitoring and Analysis

Introduction
- Introduction to Incident Monitoring and Analysis (Static and Dynamic)
- Static Analysis in the SOC
- Dynamic Analysis in the SOC

Lesson 5 — Risk Tolerance and Prioritization

Introduction
- Using Exposure to Calculate Risk Tolerance
- Mapping and Weighting of Exposures to CVEQ Visibility Controls
- Calculating Cyber Risk Tolerance

Lesson 6 — Reporting to the Board and Exco

Introduction
- Introduction to stakeholder reporting
- Reporting to the Board and Exe. Comm (Exco)

Cybersecurity Scorecard
- Inherent Risk Profile Statement
- Risk Appetite Statement
- Benchmarking and Maturity Statement
- Visibility Statement
- Deficiency Statement
- Breach Exposure Statement
- Incident Trending Statement
- Risk Tolerance Statement

Course Feedback From Previous Participants

I really enjoyed this workshop and the case studies referenced. Sometimes technical discussions can be difficult to deal with but the facilitator found simple ways of explaining technical terms. They were understanding and accommodating.

TANZANIA REVENUE AUTHORITY

The level of student participation was excellent (usually instructors do too little or too much). The pace of the course was consistent and appropriate. I appreciate the local scenarios and case studies. Keep it up.

Equity Bank Group, Kenya

EQUITY

The instructors were excellent in explaining the concepts of the cyber security, risk quantification and related concepts. Although the theories were hard to comprehend initially, they made it seem so easy.

ሕብረት ባንክ አ.ማ.
UNITED BANK S.C.
United Bank of Ethiopia

I enjoyed the workshop! I learned a lot about cyber risk management and related exposures - fraud, data breaches and sabotage. I also found out that there are many of the technical cyber security problems can be simplified and explained in simple English . Thank you!!

Britam Insurance, Tanzania

Britam
With you every step of the way

I enjoyed the course. The material was presented in a manner that was easy to understand and also easy to implement in my organization.

Office of Auditor General, Botswana

OAG

This class was very enjoyable and I will definitely recommend this workshop to my other peers who have not yet taken attended this workshop. The class exposed me to new techniques of communicating to Senior management and Board on Cyber security issues.

Kenyatta National Hospital, Kenya

KNH

The facilitators of this workshop have taken difficult technology issues and broken them down into understandable content. Even though the course was only for a week, the case studies and group work made it easy to understand the subject.

Office of Auditor General, Ghana