CVEQ™

Cyber Risk Visibility & Exposure Framework Workshop

Gaborone

Eligible and Certified ISACA Participants Will Earn CPE Hours

Organised and facilitated by;

African Cyber Security

SERIANU

Workshop Overview

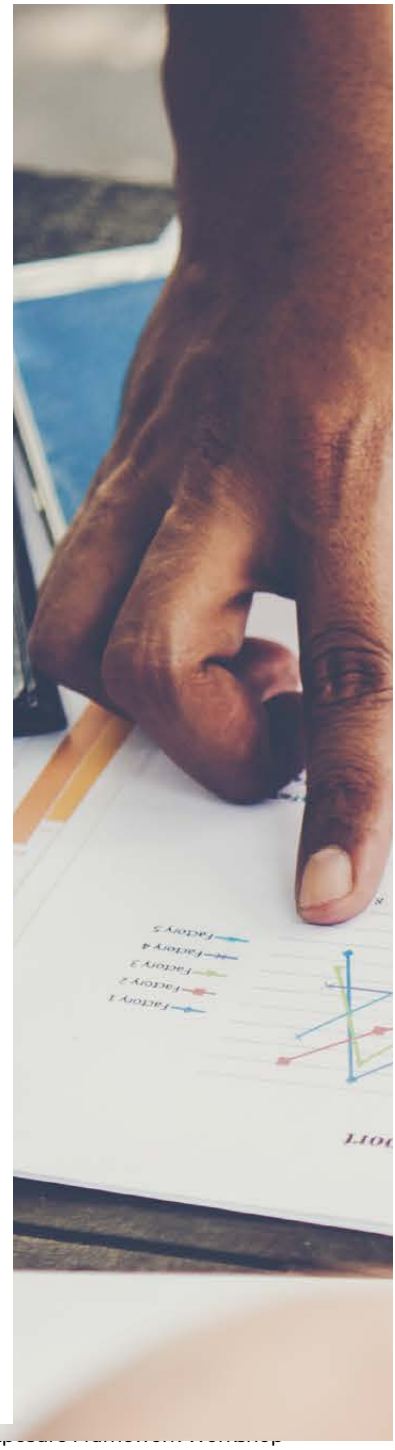
P15,000

Cost Per Delegate
exclusive of taxes, travel
and accommodation costs

50+
Attendees

5
Days

11
Sessions



Cybersecurity is a critical but often misunderstood aspect of an organisation's risk management program. Many organisations are struggling with cybersecurity issues because their cybersecurity programs are underdeveloped, unfinished or non-existent.

The days of downloading policy templates from search engines and adopting these as internally approved policies are gone.

Organisations need to adopt a holistic approach that begins with an accurate overview of an organisation's risk profile and emphasis on the most likely and most threatening cyber risk scenarios, achieving a balance between effective resilience and efficient.

Workshop Overview

Workshop Summary

This workshop is a high-energy, facilitated experience that provides you with cutting-edge insights into the intricacies of cybersecurity risk management. You gain the tools you need to lead and manage your business amid the constant onslaught of cyberattacks.

Participants will gain the tools required to design, develop and implement Cyber risk management processes. We help translate the technological underpinnings of cyberspace and cybersecurity into usable principles that will strengthen an organisation's Cyber risk management approach and communicate its use of cybersecurity practices to internal and external stakeholders.

Learning Objective

The main objective of the training is to provide the participant with step-by-step guidance on how to design, develop and implement Cyber risk management capabilities. Implementing these processes as per the guidelines in this training enables an organisation to strengthen its Cyber risk management approach and communicate its use of cybersecurity practices to internal and external stakeholders.

Specific Objectives

1. Learn how you can establish and implement Cyber risk management accountability and oversight structures;
2. Understand how to develop and implement risk controls and countermeasures that effectively and aggregately reduce the likelihood of a malicious actor successfully breaching it;
3. Discuss how to develop and implement appropriate capabilities to effectively identify, analyze, prioritize and respond to potential cyber threats; and,
4. Learn how to develop and implement appropriate metrics and measurements to represent the risk posture that can easily communicate to management and Board.

Target Audience

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

Workshop Schedule

	DAY ONE	DAY TWO	DAY THREE	DAY FOUR	DAY FIVE
	CYBER RISK LANDSCAPE AND RISK PREPAREDNESS	**RISK REDUCTION AND CONTROL FRAMEWORKS**	EXCURSION	**RISK DETECTION AND THREAT MODELLING FRAMEWORKS**	**RISK EXPOSURE ANALYSIS AND MANAGEMENT**
9:00 – 10:00	Emerging Threats, Trends and Challenges	CVEQ Risk Reduction Process		CVEQ Risk Detection Process	Current Risk Exposure Profile Scoring and Reporting
10:00 – 10:45	Cybersecurity Risk Frameworks	Cybersecurity Control Frameworks		Threat Scenarios and Indicators	Target Risk Exposure Profile Definition and Remediation Planning
10:45 - 11:15	**TEA**			**BREAK**	
11:15 – 11:45	CVEQ Risk Preparedness Process	Risk Oversight and Governance		Threat Indicators Assessment	Remediation Implementation and Reporting
11:45 – 1:00	Business Scoping and Inherent Risk Analysis	Control Framework Design and Implementation		Threat Detection Capability Assessment and Reporting	Continuous Assessment and Improvement
1:00 – 2:00	**LUNCH**			**BREAK**	
2:00 – 2:45	Data Profiling and Risk Scenario Analysis	Control Framework Monitoring and Evaluation		Threat Detection Capability Assessment and Reporting	Group Presentations and Case study Discussions
2:45 – 3:30	Case Study – Mega Africa, Bangladesh Bank	Case Study - Mega Africa, Bangladesh Bank		Data Privacy Laws and Privacy Principles	Group Presentations and Case Study Discussions
3:30 – 4:00	Cybota – Risk Profile Analysis and Reporting	Cybota – Control Effectiveness Assessment and Reporting		Cybota – Threat Exposure Analysis and Reporting	Workshop Closure and Feedback

Workshop Content Summary

DAY 01

Cyber Risk Landscape and Risk Preparedness

Participants will learn about the local and global threat landscape; how to conduct detailed risk analysis, identify and understand the amount of risk posed to the organisation by its operational activities; reviewing the organisation's risk governance and oversight practices to determine if the leadership has the appropriate skills, resources, and approach in place to minimize the likelihood of an incident and the ability to mitigate the damage should one occur.

DAY 02

Risk Reduction and Control Frameworks

Participants will be taken through the process of measuring the effectiveness and efficiency of implemented technical and process cybersecurity controls within an organisation. 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 04

Risk Detection and Threat Modelling Frameworks

Participants will learn how to conduct a detailed assessment and analysis of the organisation's threat detection processes to validate the organisation's internal capability to accurately and effectively detect potential threat events and malicious activities; determine the organization's practices around IT asset health, user management and configurations management; and, determine the availability of threat data to enable the organisation to detect observable malicious threat indicators, behaviours and anomalies.

DAY 05

Risk Quantification and Exposure Analysis

Participants will learn how to evaluate the organisation's current risk profile (Risk maturity and exposure levels) and determine the desired target risk profile; identify and prioritize mitigation of identified gaps based on existing risk management practices; and, establish consistent and detailed tracking of remediation plans to ensure the organisation is monitoring the status of remediation efforts through completion and that implemented changes are appropriately addressing risk.

Workshop Content Description

LESSON 1:

Business Profile Analysis and Scoping

This topic focuses on identifying the strategic objectives and priorities of the implementing organisation. This assists the organisation in determining the breadth and scope of the implementation.

- Identify the organisation's core business objectives and priorities,
- Identify and prioritize key operational activities or services,
- Identify the scope and level of digitization in the organisation,
- Determine the level of dependency on external service providers.

LESSON 2:

Inherent Risk and Data Profile Analysis

This topic focuses on conducting a detailed risk analysis, identifying and understanding the amount of risk posed to the organisation by its technologies and connections, delivery channels, products and services, organisational characteristics, and external threats, notwithstanding the organisation's risk-mitigating controls

- Identify and prioritize the top sources of Cyber risk in the organisation.
- Identify and prioritize the different types of data collected, stored, and processed by the organisation.
- Identify and prioritize possible Cyber risk events that the organisation is exposed to.
- Identify and prioritize possible cyber threat events that the organisation is exposed to.

LESSON 3:

Risk Governance and Oversight

This topic focuses on reviewing the organisation's risk governance and oversight practices to determine if the board and management have a clear perspective on how the business could be most seriously impacted, and that leadership has the appropriate skills, resources, and approach in place to minimize the likelihood of an incident and the ability to mitigate the damage should one occur.

- Determine the completeness, adequacy and appropriateness of the organisation's risk management and governance practices, policies and procedures. The review should focus on the following categories governance, risk management, resources, third parties and sensitive data.

LESSON 4:

Control Design and Implementation

This topic focuses on ensuring the organisation develops and selects control options that will reduce the risk for the organisation. The focus is on ensuring that the organisations implement actions that will often result in improved controls and greater control effectiveness.

- Identify and define risk scenarios/control gaps and the extent and scope of controls needed to reduce risk.
- Communicate and validate proposed control options with key stakeholder's risk owners and control owners.

Workshop Content Description

LESSON 5:

Control Framework Monitoring and Evaluation

This topic focuses on performing detailed analysis and evaluation of the organisation's Cybersecurity Control Framework to determine if they are designed correctly and if they are effective in reducing or managing Cyber risk exposure.

- Determine the effectiveness of the organisation's risk management activities and Cyber risk control framework based on asset controls, user controls, incident controls and continuity controls.

LESSON 6:

Threat Detection Capability Assessment

This topic focuses on conducting a detailed assessment and analysis of the organisation's threat detection processes to validate the organisation's internal capability to accurately and effectively detect potential threat events and malicious activities.

- Determine the organisation's practices around IT asset health, user management and configurations management.
- Determine the availability of threat data to enable the organisation to detect observable malicious threat indicators, behaviours and anomalies.

LESSON 7:

Data Privacy Laws and Privacy Principles

This topic focuses on legal implications of the local laws, processes to put in place for compliance.

- Privacy origins, GDPR/Africa Union & Kenya Data Protection Background.
- Data privacy and protection principles.
- Cyber threats landscape review and data protection gaps.

LESSON 8:

Current Risk Profile Analysis

This topic focuses on analysing the organisation's practices and capabilities to determine if the organisation is implementing their Cyber risk program as expected and achieving its intended outcomes. This helps the organisation determine the extent to which Cyber risk management is informed by business needs and is integrated into an organisation's overall risk management program.

- Determine the risk maturity level (process capability maturity and practice capabilities maturity) of the organisation's Cyber risk management capabilities.
- Determine the risk exposure level (risk profile, control effectiveness and threat detection capability) of the organisation based on its Cyber risk management capabilities.

LESSON 9:

Risk Profile Validation and Reporting

This topic focuses on compiling existing gaps, developing communication reports and presenting these to a wider audience within the organisation. These reports should be validated by internal stakeholders and provide specific recommendations for the improvement of the organisation's cyber security Program, including, where applicable, suggestions concerning the organisation's policy and procedures, governance structures, security strategies, training and resources.

Workshop Content Description

- Compile all identified gaps and share draft reports with key process owners for validation.
- Provide recommendations for the improvement of the organisation's Cyber Risk Program.
- Prepare final reports and presentations to key stakeholders and decision-makers.

LESSON 10:

Target Profile Definition and Analysis

This topic focuses on evaluating the organisation's current risk profile (Risk maturity and exposure levels) and determining the desired target risk profile. This enables the organisation to identify and prioritize mitigation of identified gaps based on existing risk management practices, the current risk environment, legal and regulatory requirements, business and mission objectives, and any other applicable organisational limitations.

- Review and analyse the current risk profile and determine the desired future risk profile.
- Identify and prioritize key remedial actions and initiatives that will enable the organisation to reach the desired Cyber risk posture profile.
- Determine and allocate adequate resources to ensure the target risk profile can be achieved.

LESSON 11:

Risk Remediation Planning and Implementation

This section focuses on rationalizing and developing remediation options and assembly of remediation plans to address identified control gaps, including quantifying the timeline requirements for each remediation project and designing a remediation roadmap.

- Group identified gaps in remediation projects based on the types and nature of mitigating controls.
- Coordinate with other business units to understand potential synergies with other business and IT projects.
- Prioritize and organize recommended projects into a phased remediation roadmap with clear timelines.
- Prioritize recommended projects into a phased remediation roadmap, including timing, duration of projects, as well as inter-dependencies.

LESSON 12:

Risk Remediation Tracking and Monitoring

This section focuses on establishing consistent and detailed tracking of remediation plans to ensure the organisation is monitoring the status of remediation efforts through completion and that implemented changes are appropriately addressing risk. Tracking of remediation efforts ensures that the organisation is aware of the status of action plans and effectively managing risk.

- Highlight the status of remediation activities and implementation for the key risks noted in the assessment phase.
- Assess the adequacy of the Cyber risk remediation efforts in meeting and supporting the attainment of the organisation's strategic objectives.
- Provide management assurance that the remediation implementation process was followed and completed efficiently.

CVEQ™

Cyber Risk Visibility & Exposure Framework Workshop

TBA

Gaborone

REGISTRATION FORM

Please complete this form by typing or printing in capital letters. Use English character and abbreviation only if more than 40 characters and space per line.

For multiple registrations, you can make a copy of the form. Remember to enclose payment and passport photo.

Upon completion, scan the registration form and email to info@africancyber.com, PRINT your names as you want it to appear on your certificate.

Designation (Tick one)	Mr	Mrs	Ms	Dr	Prof	Hon
Last Name						
First Name						
Department						
Title						
Name of Organisation						
Address				**Code**		
Office Phone				**Fax**		
Mobile Number						
Office Email						
Personal Email						

MODE OF PAYMENT

Submit your payment and return with the signed form.

- CHEQUE (Cheque No:) ◯
- INVOICE (Invoice No:) ◯
- EFT (Scan bank transfer document) ◯
- CASH PAYMENT ◯

PAYMENTS

Workshop Fees

Pula: 15,000

Add Government Taxes.

This Fees includes tuition, certification, copy of CD with presentations slides, and conference services i.e. AM/PM Tea/Coffee with assorted snacks, water and buffet lunch.

For more information, please call:

Mareledi: +267 77 008 852 / +267 3980390

EARLY BIRD REGISTRATION - 10% DISCOUNT IF YOU PAY NOW.

BULK BENEFITS - BOOK FOR 2 OR MORE DELEGATES AND GET 5% DISCOUNT ON THE QUOTED PRICING.

BANK DETAILS (FOR E.F.T)

Bank Name: First Capital Bank - Botswana

Account Name: African Cyber Security

Account Number: (PULA: 0002704012855

Account Number: (USD): 0002703010649

Branch: Main

Swift Code: FRCGBWGA

BOOKING CONFIRMATION

Yes I Will attend	◯	**No I Will Not**	◯
Signature			
Date			
Undecided - state possibility			

TERMS AND CONDITIONS

- **A signed registration form, returned to African Cyber Security Limited office indicates that you have read and agreed to the terms and conditions set out below:**
- **A place on any course is reserved only upon receipt of a signed training registration form accompanied by a purchase order for an amount equal to the quoted course fee.**
- **Full payment for all training activities must be received 7 working days prior to the commencement of the course.**
- **African Cyber Security Limited reserves the right to cancel or re-schedule courses with 7 days notice. In the event of such cancellations, registrants can opt to have all the pre-paid fee refunded in full or credited towards the next available courses.**
- **In the event of customer cancellation, Course fees shall be refunded in full provided at least 14 days notice is given prior to course commencement. No refunds will be given in respect to customer cancellation received less than 14 days prior to commencement of the scheduled course.**
- **African Cyber Security Limited reserves the right to change the speaker, venue, date and vary/cancel the program should circumstances beyond its control arise. Serianu Limited also reserves the right to arrangement without prior notice should it be necessary to do so.**
- **Thank you for your interest in Afrcan Cyber Security Limited training services.**

Note:
At some events, we will have a photographer present.
Please tick this box if you do not wish to be photographed.

AUTHOURIZATION

This booking is NOT valid without a signature. The signatory must be authorized to sign on behalf of contracting Organisations. Name of authorizing Officer:

Name of authorizing Officer:

Signature: **Date:** **Email:**

Organised and facilitated by;

African Cyber Security

FOR FURTHER ENQUIRIES

Email: info@africancyber.com or **Call:** Mareledi +267 77 008 852 / +267 3980390

African Cyber Security (pty) Ltd
Unit 3, The Office, Fairgrounds,
Gaborone

General Information:

+267 77 008 852
+267 3980390

info@africancyber.com

https://www.africancyber.com