

EAST AFRICAN CYBER SECURITY SUMMIT 2015

Developing Sustainable and Synergetic Strategies in a Digital World.

22nd to 24th July 2015

Intercontinental Hotel
Nairobi, Kenya

**THE FIRST 10
DELEGATES TO BOOK
BEFORE 8TH MAY WILL
GET FREE TABLE PC
BOOK & PAY NOW !**



EARLY BIRD BOOKING DISCOUNT
PRICES EXCLUDES VAT WHERE APPLICABLE

1. BEFORE 30TH APRIL USD 890
2. BEFORE 30TH MAY USD 990
3. 3 DELEGATES AND ABOVE USD 890

ABOUT THE SUMMIT

According to computer security experts, a lot of cyber-crime emanates from the African continent, and these threats spread easily because many computer systems are not properly protected. The fight against cybercrime requires a cohesive and coordinated approach, but in Africa, poverty and underdevelopment are the major causes for growth of cybercrime in the region.

The potential for internet abuse in Africa is also high. This is due to the lack of security awareness programs or specialized training for the law enforcement agencies.

Global reports indicate a rise in computer crime, referred to as cybercrime or computer crime. Consequently organizations lose billions of dollars annually. In banking sectors in East Africa, billions are deemed to have been lost due to failure of ICT Security Controls.

As East Africa is now moving onto the digital age with cashless payments of fare, tax and others, needs to be conducted on the dangers of such software. Experience shows that organizations with proactive information security approaches reduce the chances of loss due to cybercrime.

WHY YOU SHOULD ATTEND

1. **Exclusive Attendee List:** Attendees from various industries have the opportunity to have in-depth conversations about industry pain points and best practices.
2. **Networking Opportunities:** Build a network of peers capable of providing you with invaluable business advice with which to grow your career.
3. **Intimate Environment:** The Summit will create opportunities for valuable conversations with analysts in a comfortable, yet focused business setting.
4. **Invest your time in our event** and we'll ensure that you leave with invaluable information that will help move your organization ahead of the competition.
5. **Learning Opportunity:** Agenda sessions at the Summit are led by leading executives speaking on topics aligned with their knowledge and expertise.

WHO SHOULD ATTEND

- » Business Analysts
- » Director Generals and Deputy Director Generals
- » CIOs and CISO's
- » Information Security managers and directors
- » Information Security staff administrators
- » New to COBIT, want to learn more about COBIT 5
- » IT professionals in IT audit, advisory and risk.
- » Enterprise security architects
- » Data security professionals
- » Internet Security Managers
- » Systems Planners and analysts.
- » Security analysts
- » Software and application developers
- » Engineers
- » Technical and Support specialists
- » Systems Integrators
- » New to COBIT, want to learn more about COBIT 5
- » Director Generals and Deputy Director Generals
- » Enterprise security architects
- » Data security professionals
- » Internet Security Managers
- » Systems Planners and analysts.
- » Technical and Support specialists
- » Systems Integrators
- » Web Masters

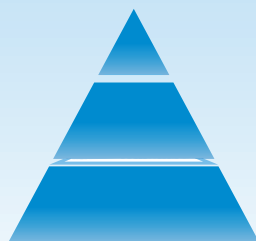
WE ARE ACCREDITED BY:
THE NATIONAL INDUSTRIAL TRAINING AUTHORITY
NITA/TRN/870

Access Business Management International
ABMC International

Head Office: Nairobi, Kenya
45 Westlands Road, Leomar Court, Suite No. 10
Tel No.: +254 20 3742004/2005/2024

Email: info@intl-abmc.com

www.intl-abmc.com



A.B.M.C INTERNATIONAL LTD

ACCESS BUSINESS MANAGEMENT CONFERENCING INTERNATIONAL LTD
LEADERS IN BUSINESS TRAINING



Summit Program

DAY 1 22nd July 2015



Angela Nganga - Corporate Affairs Lead For East And Southern Africa & Indian Oceans Islands, Microsoft.
BE PREPARED WHEN THE VICTIM IS YOU: HOW TO PREPARE YOUR BUSINESS CONTINUITY MANAGEMENT SYSTEM



Charles Mbuvi - Head Of Security, Vivo Energy.
FIGHTING CYBER CRIME IN AFRICA AND HOW TO RECOVER AFTER AN ATTACK-"THE EAST AFRICAN PERSPECTIVE"

Felix Mulei - Banking ICT Consultant, (Eclectics International)
HOW COMPANY LEADERS CAN PROTECT AND STRENGTHEN THE BUSINESS WITH THE RIGHT APPROACH TO INFORMATION SECURITY



Michael Mbuthia - Head IT Risk & Controls-Co-operative Bank of Kenya
HOW TO HANDLE THE INSIDER THREAT: PROFILING CYBER CRIMINAL BEHAVIOUR.

PANEL DISCUSSION-KENYA CYBER SECURITY ACT 2013

DAY 2 23rd July 2015



Erick Mugo - Head IT Security, Chase Bank
ONLINE AND MOBILE BANKING INFRASTRUCTURE UNDER THREAT: UNDERSTANDING CYBER THREATS



Alexander Fine-Director-Odin South Africa
Cloud Security-Understanding the risks Involved



Joseph Nyabok - Head Of IT Security, CFC Stanbic Bank
A PLATFORM APPROACH TO STOP CYBER THREATS TO INDUSTRIAL CONTROL SYSTEMS, FROM EMERGING CYBER THREATS.



DR. MATUNDA NYANCHAMA PHD, CISSP-CONSULTANT, AGANO CONSULTING
E-GOVERNMENT: GOVERNMENT AND BUSINESS WORKING TOGETHER TO COUNTER CYBER THREATS.

Yusuph Kileo-Cyber Security and Digital Forensics Expert, Tanzania
THE HACKERS NIGHTMARE - FUTURE TRENDS IN DIGITAL FORENSIC INVESTIGATION AND ADVANCED REPORTING SYSTEMS

DAY 3 24th July 2015

MASTERCLASS WORKSHOP



Tichaona Zororo
Director, Egit Enterprise Governance Of IT CIA, CRMA, CISA, CISM, CRISC, CGEIT

Exploring the Business Impact of Cybersecurity & Implementing the NIST CSF Using COBIT 5
The Governance & Management of Digital Vandalism

WORKSHOP OUTLINE

Today's cybersecurity attacks portend more threatening ones ahead as evidenced by recent disruptive DOS against the US financial industry that hampered 15 of the largest US banks for hundreds of hours. Major enterprises like Target, Home Depot and Sony Entertainment experienced breaches that required the companies to pay hundreds of millions of US dollars to cover costs of the attacks.

While these enterprises shared the similar misfortune of experiencing incidents, the incidents themselves were not all the same. In the cases of Home Depot and Target, intrusion initially occurred via hacked third-party vendors and financial gain was the motivation. Sony was the victim of extremely sophisticated malware that was used to steal confidential information. As breaches become more significant, they cause increased financial impact.

Cyberattacks also known as digital vandalism have increased in both frequency and impact. Organizations are no longer asking "are we secure?" but "how can we ensure that the information most important to our business will be secure enough?" The best-prepared businesses now recognize that responsibility for deflecting cyber attacks is no longer just the responsibility of their IT departments; it is an enterprise-wide boardroom issue. The only sure way to counter the threat is with an approach that roots the organization's cybersecurity strategy in the real world of its business strategy.

The ISACA Guide to Implementing the NIST Cybersecurity Framework provides guidance in the implementation of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) through a seven-step process, aligned with COBIT5 principles.

It is aimed as a further level to the COBIT5 Foundation Qualification, alongside the COBIT5 Implementation Practitioner and COBIT5 Assessor Practitioner.

Meet Our Workshop Speakers



Tichaona Zororo

**Director, Egit Enterprise Governace Of IT
CIA, CRMA, CISA, CISM, CRISC, CGEIT**

Tichaona Zororo is the Vice President and Program Coordinator ISACA South Africa, an Audit Committee Member of KZN Legislature, Eastern Cape Province Department of Roads & Public works and Setsoto Local Municipality and a Member of ISACA International's Framework Committee charged with identifying and supporting activities required to appropriately define, build and maintain a globally applicable and practically useable ISACA enterprise governance and management of IT (GEIT) framework (COBIT).

He has served on the ISACA international CGEIT Test Enhancement Sub Committee and External Advocacy Committee.

He is an IT advisory and assurance Executive with vast years of in-depth experience in mainstream IT, IT auditing, IT Governance and IT Risk across private and public sectors in the USA, Belgium, UK, India and numerous countries across Africa.

Tichaona Zororo is Director IT advisory with EGIT | Enterprise Governance of IT an IT Advisory firm and COBIT 5 Accredited Training Organisation based in South Africa focusing on advising the Board, Senior Business Executives and Management, IT Auditing, IT Governance Advisory and Enterprise Risk Management. He is an advisor to numerous boards and executives in Africa and abroad on Emerging Technologies, Enterprise Governance and Management of Enterprise IT, IT Risk, IT Security and IT Auditing. He is Chairman IT Committee of Eastern Cape Province Department of Roads & Public works.

He is a sought after trainer, speaker and published author in IT Governance, COBIT 5, IT Auditing, Social Media, Cloud Computing, Big Data, Cyber Security and a renowned COBIT 5 subject matter expert and accredited trainer who has participated in the review and development of numerous COBIT 5 publications, ISACA white papers and audit programs.

Tichaona Zororo is a Certified Internal Auditor (CIA), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Certified in Risk Management Assurance (CRMA), Certified in Risk and Information Systems Control (CRISC), Certified in Governance of Enterprise IT (CGEIT) and Certified COBIT 5 Assessor. He Holds a B.Sc. Honours Information Systems (MSU), A Post Graduate Diploma in Computer Auditing (Wits) and several other certificates in business and IT.

He is credited for being the first COBIT 5 Certified Assessor in South Africa and the 40th internationally. Tichaona is an accredited COBIT 5 Foundation, Implementation and Assessor qualifications trainer.



Yusuph Kileo

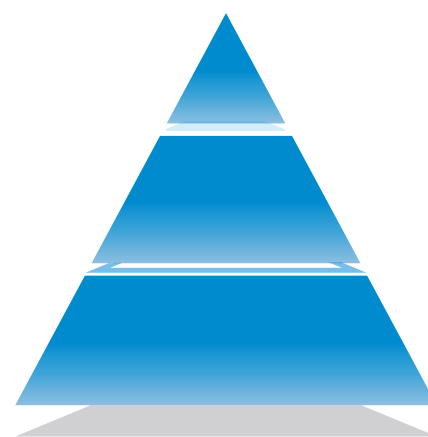
**Cyber Security and Digital Forensics Expert,
Tanzania**

Yusuph Kileo is an expert in the fields of cyber security and digital forensics. Yusuph started developing his IT skills while working with Brand East Africa in 2006. In 2008 he joined the MIS department at the Tanzania Telecommunication Company where he developed his interest in the security field. In 2010 he joined Deloitte's IT department where he further strengthened his security skills.

In 2012, Yusuph joined the Tanzanian Government's Criminal Investigation Department (CID) as a cyber-security and digital forensics investigations expert.

The CID falls under the Forensics Bureau section which is focused on cybercrimes. During his time with the cybercrime unit he conducted several training sessions and provided insights on cyber challenges in Tanzania.

He is often invited to speak or chair information security, risk, and crime sessions as well as provide opinion pieces via TV, radio and print and / or online media. He is currently an adviser for cyber-security matters in Tanzania.



A.B.M.C INTERNATIONAL LTD

ACCESS BUSINESS MANAGEMENT CONFERENCING INTERNATIONAL LTD

LEADERS IN BUSINESS TRAINING

**Access Business Management International
ABMC International**

Head Office: Nairobi, Kenya
45 Westlands Road, Leomar Court, Suite No. 10
Tel No.: +254 20 3742004/2005/2024

Email: info@intl-abmc.com
www.intl-abmc.com

Registration Form

To register, please provide the following information and send this form to karen@intl-abmc.com

NAIROBI OFFICE: +254(020)3742004/2005/2024/2043

1. Dr. Mr. /Miss/Mrs.....Cell.....
Department.....Position.....Email.....
2. Mr. /Miss/Mrs.....Cell.....
Department.....Position.....Email.....
3. Mr./Miss/Mrs.....Cell.....
Department.....Position.....Email.....
4. Mr./Miss/Mrs.....Cell.....
Department.....Position.....Email.....

EARLY BIRD BOOKING DISCOUNT-PRICES EXCLUDES VAT WHERE APPLICABLE

Prices not inclusive of accommodation and flights

- ☐ 1. BEFORE 30TH APRIL USD 890 ☐ 2.BEFORE 30TH MAY USD 990 ☐ 3. 3 DELEGATES AND ABOVE USD 890

AUTHORIZATION

Signatory must be authorized to sign on behalf of contracting organization, any cancellation should be done in writing 30days before the training dates there after 100% course fee will be charged , a substitute will be accepted .This booking is invalid without a signature.

Name:.....Cell/D Line:.....Job Title:.....

Email.....Organization.....

VAT No.....

TelephoneFacsimile.....

Physical Address.....

Postal Address.....

SIGNATURE:.....REGISTRATION DATE...../...../.....