

Kabuthia Riunge - CISSP, CRISC, CISM, CISA

PO Box 50114 Nairobi – 00100, Kenya.

Cell phone: +254.722.843.818 email: kabuthia.riunge@gmail.com

Date of Birth: 27th July 1978

Nationality: Kenyan

Career Objective:

Seeking a leadership position where I will lead a team of professionals to follow a risk-based approach in evaluating technologies, designing technical architectures and developing & implementing strategies to enable the organization create value for its stakeholders through benefits realization and resource optimization.

Education:

Academic:

Sept 2018 – date	Master of Science, Information Security University of London
May 2013 – March 2014	Diploma, Risk Management in Finance and Banking Sida/KPMG - Sweden
July 2006 – June 2007	Diploma, Project Management Kenya Institute of Management
April 1998 – Nov 2003	Bachelor of Science, Electrical and Electronic Engineering Jomo Kenyatta University of Agriculture and Technology
Jan 1993 – Nov 1996	Kenya Certificate of Secondary Education (KCSE) Starehe Boys' Centre and School

Professional:

July 2019	Certified ISO/IEC 27001 Lead Implementer Certificate Number: ISLI1043972-2019-07
Sept 2018	Certified in Risk and Information Systems Control (CRISC) CRISC certification number: 1824758
Feb 2011	Certified Information Security Manager (CISM) CISM certification number: 1115734
June 2010	Certified Information Systems Security Professional (CISSP) CISSP certification number: 371837
May 2010	Certified Information Systems Auditor (CISA) CISA certification number: 1083565

Successfully completed the following courses of instruction and learning, among others:

- Computer Hacking Forensic Investigator v9 (AFRALT – Feb 2019)
 - Managing Computer Security Incident Response Teams (Carnegie Mellon University – March 2018)
 - Checkpoint Certified Security Expert (Arrow ECS, London UK – July 2013)
 - AIX System Administration I and II (Tricon Academy – October 2010)
 - Implementing Cisco NAC Appliance – CANAC (Global Knowledge, UAE – Sept. 2010)
-

Professional Associations:

- Current Chairman – IT Risk and Security Subcommittee at Kenya Bankers Association (**KBA**)
- Founder President of **(ISC)² Kenya Chapter**
- Member of International Information Systems Security Certification Consortium, **(ISC)²**
- Gold level member of **ISACA**
- Vice Chairman – IT Risk and Security Subcommittee at KBA – 2017 /2018

Professional Accomplishments:

- Built the Information Security Risk Department at NIC Group from the ground up.
 - Mentor, teacher and trainer on information security. Leading a team of information security professionals volunteering to train children on how to be safe and secure online, and be responsible digital citizens.
 - Led the team that designed and implemented the Security Management System in T24 core banking system (CBS) upgrade project (R11 to R17) at NIC Bank.
 - Led the team that designed and implemented the Security Management System in T24 CBS for the Central Bank of Kenya (CBK).
 - Team leader for the design and implementation of PKI based security for the Internet Banking Solution at CBK.
 - Project manager for the Internet Perimeter Security Upgrade Project in which we successfully implemented a fully redundant appliance architecture with defense in depth and DMZ features at the CBK's multiple data processing facilities.
 - Team leader for a Data Loss Prevention and end-point encryption project implemented through Kaspersky Security products at CBK.
 - Successfully implemented a Cisco Network Admission Control System across all branches and currency centres of CBK.
 - Contributed to the drafting of the Kenya National Cybersecurity Framework at Communications Authority of Kenya.
 - Project manager for the successful ISMS initiation project in Mumias Sugar Company which included a gap analysis, risk assessment and a subsequent risk treatment plan, and an ISMS framework in compliance with ISO/IEC 27001.
-

Professional Experience

April 2012 to date: **National KE-CIRT/CC Cybersecurity Committee (NKCC) - Kenya Member**

Duties and responsibilities:

- Advising and coordinating computer security incident response at the national level and acting as a national trusted point of contact.
 - Liaising with the local sector Computer Incident Response Teams (Sector CIRTs), regional CIRTs, international CIRTs and other related organizations.
 - Gathering & disseminating technical information on computer security, incidents, vulnerabilities & security fixes.
 - Carrying out research and analysis on computer security, related technologies and advising on new trends.
 - Overseeing the implementation of a national Cybersecurity Masterplan
 - Facilitating the deployment of a national Public Key Infrastructure framework.
 - Identifying Kenya's critical infrastructure and providing ways to protect it.
 - Capacity building in information security and creating and maintaining awareness on cybersecurity-related activities; among others.
-

July 2010 to date: **ISACA and (ISC)²
Training facilitator, speaker and presenter**

I am a part-time trainer for CISA, CISM and CISSP certification programs ran by Kenya Chapters of ISACA and (ISC)².

I also speak and make presentations at national and international information security conferences.

Dec 2014 to date: **NIC Group PLC
Head, Information Technology Risk**

- Coordinating activities to direct and control NIC Group with regard to information technology risk.
- Member of the NIC ICT Steering Committee, the highest ICT decision making organ in the group, and which reports to the Board ICT Committee.
- Consistently and comprehensively reporting results of risk monitoring and control actions to senior management, the board and regulators in accordance with CBK Risk Management Guidelines (RMGs) & Guidance Notes (GNs).
- Established effective mechanisms to identify; assess; respond & mitigate; and control, monitor, & report information security risks inherent in the Group's ICT infrastructure comprising hardware & software systems, data, and communications networks.
- Safeguarding the confidentiality, integrity, availability & consistency of data.
- Providing relevant early warning mechanisms to enable proactive corrective actions to prevent information security risks from materialising.

- Developing and implementing extensive information security awareness and training programs to promote a strong culture of sound information security risk management and compliance in the group.
- Developing and documenting technology strategies to restore hardware, applications and data in time to meet the needs of business recovery.
- Monitoring emerging risks and changes to laws and regulations and standards.
- Collaborating with system administrators and others charged with safeguarding the information assets of the bank to ensure appropriate control design.
- Maintaining comprehensive information security risk registers.
- Ensuring the implementation of information security risk management strategy.
- Ensuring that a comprehensive inventory of ICT assets, classified by business criticality, is established and maintained through a regular Business Impact Analysis (BIA) process.
- Conducting red team exercises.

July 2010 to Nov 2014: **Central Bank of Kenya (CBK)**
 Senior Information Security Officer

I was responsible for protecting the Bank's IT resources and information assets by:

- Ensuring tactical implementation of information security in support of business objectives.
- Ensuring Availability, Confidentiality, Integrity, Audit-ability of the Bank's information systems.
- Ensuring reduction of adverse impacts on the Bank's business operations to an acceptable level.
- Ensuring conformity to applicable laws, regulations and standards.
- Ensuring non-repudiation of computer-based activities.

Specific duties and responsibilities

- Processed requests to grant application and network access privileges that have been approved by appropriate authorities.
- Maintained and updated the configuration of endpoint protection systems, intrusion prevention systems, intrusion detection systems, firewalls, and other deployed security systems within the Bank.
- Participated in information security incidents response activities.
- Preserved all records indicating changes made to access control lists.
- Executed automated mechanisms that analysed security violations found in access control logs to discover patterns and evidence of problems.
- Monitored security logs of computers, network and security devices to detect attempts of unauthorized access, and notified management as necessary.
- Implemented information security policies, standards and procedures.

- Maintained an inventory of all information security requirements documents such as policies, standards, and procedures, etc. Distributed these documents and maintained an intranet site that reflected the current version of all these documents.
 - Developed, implemented and monitored an information security awareness and education program across the Bank to effectively communicate and raise awareness of the security policies and the potential impact of security incidents.
 - Provided technical assistance to IT administrators in their efforts to implement security controls in various systems and in monitoring access and usage of the systems.
 - Provided bank staff with technical support on matters related to information security.
 - Performed information security risk assessments on IT Systems.
-

Sept. 2007 to June 2010: **Mumias Sugar Company Limited (MSC)**
IT Security Administrator

- Planning, designing, implementing and maintaining security programs, policies and procedures in all computer based information systems.
 - Ensuring that the user community understands and adheres to necessary procedures to maintain security through user privacy and security awareness & education programs.
 - Conducting accurate evaluation of the level of security required by carrying out risk assessment on ICT systems & identifying information security risks and exposures.
 - Harvesting, monitoring, analysing and archiving logs from applications, operating systems, databases and security appliances.
 - Responsible for back-up regimes for all electronic data. I was a key member of the ICT Business Continuity Planning team. I was also a member of the Incident Management and Disaster Recovery teams.
 - Managing and administering Sun Solaris clustered database and application servers hence ensuring systems were highly available.
 - Performing patch management, security management and performance optimization of endpoints.
 - Administering *McAfee Total Protection for Endpoint – Advanced*. This software comprises antivirus, antispyware, anti-SPAM, host intrusion prevention, email & web security, network access control etc.
 - Managing Cisco Adaptive Security Appliance (Firewall, VPN and IPS).
 - Maintaining two data centres by ensuring that the environment stays safe, secure and conducive for optimal performance of ICT equipment.
 - Administration of environment monitoring systems, air-conditioning, fire detection and suppression, access control, power systems, and cable management in the data centres.
 - Configuring and administering email and internet security applications (*WebMarshal* and *MailMarshal SMTP*).
 - Maintaining the disaster recovery plan including coordination of the bi-annual disaster recovery tests.
 - Liaising with contractors and service providers to ensure that Service Level Agreements are achieved in order to meet or exceed ICT users' expectations.
-

July 2006 to Aug. 2007

Mumias Sugar Company Limited
ICT Systems and Network Administrator

- I was instrumental in the transformation of MSC's campus LAN from a 200-points, flat, 10mbps hub based LAN to a 1200-point, routed, gigabit MAN. The MAN includes a wireless mesh network spanning about 800 square metres. The WAN connects three satellite branch offices. This entire network is VoIP ready with both wired and wireless VoIP phones.
 - I have extensive knowledge of and working experience with various wired and wireless networking technologies such as optical fibre, Ethernet, wireless LAN, VSAT, EDGE/3G, WiMAX etc.
 - I was a key team member in the Integrated Management Systems Project at MSC. This project led to the successful implementation of mySAP ERP system and Agricultural Management System (AMS). The invaluable experience gained went a long way in complementing my training in Project Management.
 - I set up, administered and maintained Windows Server 2003 Active Directory spanning four locations with 1500 users.
 - I set up, configured and administered MS Exchange Server 2007, Blackberry Enterprise Server, and MS Systems Management Server (SMS) 2003 Server for the domain.
 - I set up and administered enterprise antimalware, DNS, DHCP, Microsoft ISA, SurfControl etc which were not in existence in the company before.
 - I administered a Nortel call processor and signalling server which supports IP, digital, and analogue telephones.
 - I trained users and offered helpdesk support through the LanSupport helpdesk system.
-

Sept. 2004 to June 2006

K-Rep Bank Ltd
ICT Systems and Network Administrator

- I was actively involved in the bank's networking technologies especially Wi-Fi, LANs and WANs from the design stage through supervision of the installation and support after successful implementation. During my tenure, the bank grew from 3 to 21 networked branches.
- I was in charge of ensuring the availability of, and providing support for servers, PCs and other network infrastructure devices that provided connectivity for the users of the bank's IT systems.
- I developed and provided support for electronic mail systems, internet, remote access (CITRIX, Dialup, RDP, VNC), and other electronic communication devices such as PDAs and Laptop Computers that required access to the network.
- I was responsible for the design and maintenance of the bank's entire Active Directory, which spans several branches.
- I developed and ensured compliance with Security and Data Policies & Procedures.
- Provided appropriate security and access controls to the bank's ICT resources through firewalling, ACLs, antivirus software, Web filters etc.
- Monitored the usage, capacity, utilization and performance of network and server resources.
- Liaised with external vendors in providing voice, video, data and other communication services for the bank.

- Involved in research, procurement, testing and deployment of improved ICT technologies (both hardware and software) for the bank.
- Scheduled preventive maintenance of ICT equipment to ensure optimal operation at all times.

Referees:

Mr. John Wamai Director - ICT Equity Bank Group P.O. Box 75104 – 00200 Nairobi, Kenya. Cell phone: +254.763.626695 john.wamai@equitybank.co.ke	Mr. David Igweta Chief Information Officer HFC Limited Rehani House, Kenyatta Ave. Nairobi, Kenya. Cell phone: +254.722.788392 david.igweta@hfgroup.co.ke	Mr. Kasaine Ole Pertet General Manager, ICT Kenya Airports Authority P.O. Box 19001 – 00501 Nairobi, Kenya. Cell phone: +254.722.513969 kasaine.pertet@kaa.go.ke
---	---	--
