BENSON MACHARIA

CISM, CISA, CISSP, CEH, AWS, GCP | bmacharia.com | linkedin.com/in/benson-macharia | github.com/bensonmacharia

PROFESSIONAL SUMMARY

I am a Cybersecurity, Technology Risk, and IT Audit professional with over six years of experience in the financial services industry and professional services space. I specialize in designing secure applications and ensuring zero critical or high-risk issues for applications deployed to production. My expertise includes conducting comprehensive vulnerability assessments and penetration testing of enterprise applications, networks, and cloud environments. I have a proven track record of enhancing pipeline security by ensuring the complete integration of automated security testing tools in CI/CD pipelines, effectively mitigating risks and safeguarding organizational assets.

TECHNICAL SKILLS

Security Testing: Kali Linux, Metasploit, Nmap, SQLMap, Nessus, InsightVM, Burp Suite, Acunetix, MITRE ATT&CK.
Cloud: AWS Cloud, Google Cloud Platform (GCP), Azure Cloud.
DevSecOps: Docker, Kubernetes, Jenkins, Jfrog Artifactory, SonarQube, Veracode, OWASP ZAP, Acunetix, GitLab CI.
Automation: Python, Bash, PowerShell, Golang, Ansible, Javascript, Terraform, Java, PHP, C, C++, C#
Databases: MySQL, MongoDB, SQLite, PostgreSQL, Oracle, Microsoft SQL Server, DynamoDB, Cassandra, Redis.
IT Governance and Risk: COBIT, ISO/IEC 27001, NIST Cybersecurity Framework, Threat Modeling.
Internal Controls: SOX Compliance, IT General Controls (ITGC).
Reporting and Documentation: Microsoft Excel, Microsoft Access, SQL for data extraction and reporting.

WORK EXPERIENCE

Principal/Manager Cybersecurity Assurance   **Safaricom PLC (Vodafone Group Subsidiary)**

Dec 2021 - Present

- Champion adoption and integration of DevSecOps tools like Veracode and OWASP ZAP within the CI/CD pipelines for automatic security scanning, reducing software pipeline security vulnerabilities by 40%.
- Create security automation scripts using Python and Bash, resulting in a 30% decrease in manual security compliance checks on servers and database systems.
- Manage the private bug bounty program, validating all reports, awarding and facilitating closure of reports by project teams within defined SLAs.
- Conduct red team exercises on applications in production, reporting on findings and facilitating closure of all issues within SLA.
- Conduct security assessments for all waterfall and agile projects before go-live, ensuring closure of all critical/high/Medium risk defects before project go-live.
- Coordinate cross-functional teams to implement security controls and practices required by PCI DSS, resulting in the organization attaining PCI DSS certification within 6 months.
- Developed comprehensive threat models for application security reviews using methodologies such as STRIDE and PASTA to identify potential vulnerabilities and prioritize mitigation strategies, ensuring robust security postures across projects.

Assistant Manager Cybersecurity & Tech Risk Consulting   **Ernst & Young (EY)**

Feb 2019 – Dec 2021

- Conducted Central Bank of Kenya (CBK) cybersecurity compliance reviews for three leading Tier 1 and Tier 2 banks in Africa over a three-year period, facilitating closure of 95% of identified security gaps.
- Led a team of 5 cybersecurity consultants, ensuring delivery of high-quality security assessments and maintaining a client satisfaction rate of 98%.
- Managed project timelines, budgets, and resources, achieving a 95% on-time delivery rate.
- Implemented security frameworks and compliance standards such as ISO 27001, NIST, and PCI DSS, ensuring clients' adherence to industry regulations.
- Developed and delivered cybersecurity awareness training programs for clients, enhancing their security posture and reducing phishing incidents by 40%.
- Documented risk assessments and audit findings, prepared detailed reports, and presented actionable recommendations to management, aiding organizations in improving their IT governance processes.
- Assessed and tested IT General Controls (ITGC) for over 20 client systems, helping enhance internal control environments and reducing incidents.

Database Administrator   **The Judiciary of Kenya**

Dec 2016 – Jan 2019

- Led a team of 3 database administrators, managing over 10 enterprise databases running on Oracle, PostgreSQL, Mongo and MySQL database systems across multiple environments, ensuring 95% uptime through optimized maintenance schedules and proactive monitoring.
- Cordinated database backup and ensured 99.9% backup success rate by automating the backup processes and conducting regular recovery drills.
- Conducted quarterly security audits and vulnerability assessments on the databases, reducing potential security threats by 50%.
- Improved database query performance by 25% through database tuning and indexing strategies.
- Successfully led the migration of over 5TB of data from legacy case management system database to modern a database platform on Cloud with zero data loss.

Applications Developer   **World Agroforestry Centre (ICRAF)**

May 2014 – Dec 2016

- Developed a key research projects full-stack web application using JavaScript, HTML, CSS, and PHP Laravel, increasing project work visibility and research papers downloads by over 50%
- Implemented responsive design for the corporate website, resulting in a 40% increase in mobile traffic.
- Managed the migration of partners website from Joomla to WordPress, improving site performance and user experience by 60%.
- Integrated third-party services and APIs into the intranet web application, enhancing application functionality and user experience by 35%.

EDUCATION

Strathmore University	MSC. Information Systems Security	Aug 2018 – Dec 2021	Nairobi, Kenya
Kenyatta University	BSc. Computer Science	Sep 2011 – Jul 2015	Nairobi, Kenya

CERTIFICATIONS

- Certified Information Security Manager (CISM)
- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Certified Ethical Hacker (CEH)
- AWS Certified DevOps Professional
- AWS Certified Solutions Architect
- AWS Certified Developer – Associate
- Google Cloud Certified Security Engineer Professional
- Microsoft Certified Azure Security Engineer
- API Security Architect

ASSOCIATIONS

- Member of International Information System Security Certification Consortium (ISC2)
- Member of Information Systems Audit and Control Association (ISACA)
- AWS Community Builder and ISACA Mentor

PUBLICATIONS

- Personal Blog - https://bmacharia.com
- Medium - https://medium.com/@bmacharia
- Dev.to - https://dev.to/bensonmacharia
- Github - https://github.com/bensonmacharia