DOMINIC B. BOAMAH, Ph.D., CSSLP, CCSFP
2221 Lassen Drive, Prosper, TX 75078
Phone: 972-343-8530; Email: boakyeboamah@outlook.com

A seasoned and passionate Cybersecurity/IT professional with over 15 years of cybersecurity/IT engineering and leadership experience in several areas including AI security, risk management, systems integration, regulatory compliance, secure software development (S-SDLC), security engineering and automation, security architecture, third-party risk management, and breaking complex security issues down to business executives. Currently seeking opportunities in the Dallas, Texas area or remote (cannot relocate, but willing to travel).

Education:	**Certification:**
Ph.D., Capella University, Information Technology Management. M.S., University of Jyvaskyla, Finland, Information Systems.	CSSLP – ISC^2 CCSFP - HITRUST ISSAP- ISC^2 (Ongoing)

Summary of Leadership and Professional Experience:

United Airlines (Chicago, IL) – Principal Architect, Responsible AI - Security July 2024 – Present

Leading the responsible and secure design and integration of Generative AI applications into organizational systems ensuring compliance with industry standards, and evolving global regulations:

- Leading risk management and playing a leading role in technical review of all GenAI AI use cases to ensure risk mitigations, privacy considerations, and compliance with global regulations are integrated into the development process, ensuring adherence to United's Responsible AI principles, and promoting effective risk management.
- Collaborating with cross functional teams to ensure responsible, secure, and successful implementation and scalability of GenAI functionalities.
- Performing threat modeling and risk assessments of AI initiatives identifying risks, mitigations, and regulatory compliance in partnership with cross functional expert groups, and ensuring mitigations are properly implemented and functioning as required.
- Collaborating with cross functional teams to establish standardized processes for risk assessment and risk controls, streamlining risk management across all AI initiatives
- Working in close collaboration with Zscaler engineers to monitor and address unsanctioned use of GenAI tools by employees.
- Ensures compliance with internal and industry security and technological standards and best practices across all AI projects.
- Leading the review and evaluations of third-party AI tools to ensure they meet organizational requirements prior to engagement.

T-Mobile (Frisco, TX) – Principal Architect, Responsible AI - Security Mar 2023 – July 2024

Played a leadership role in the initial setup of AI policies and structures within T-Mobile:

- Led the development of organization-wide AI security standard in collaboration with the legal and privacy departments, ensuring all AI initiatives are executed in compliance with industry standards and best practices and T-Mobile's Responsible AI principles.
- Single-handedly developed T-Mobile's security architecture, strategy, and security requirements based on NIST AI 100-1, OWASP top 10 for AI, CMMC 2.0, NIST 171 r2, MITRE ATLAS.
- Developed a concept of GenAI threat model on demand based on NIST AI 100-1 and NIST.AI.600-, which made it easier for use case teams and junior engineers to identify and address potential threats in GenAI use cases.
- Played a leading role in GenAI use case architecture design and technical reviews with a security mindset ensuring privacy and security were embedded in the design, implementation, deployment, use, and maintenance of AI use cases.
- Partnered with the AI Governance team, legal, and other expert groups to continuously improve the effectiveness of risk management.
- Worked in close collaboration with T-Mobile's AI Center of Excellence (COE) team on strategic design initiatives and provided leadership in technological advancement projects.
- Guided the responsible and secure application of generative AI to deliver tangible business benefits and drive growth.
- Worked in close collaboration with the COE team to design and oversee integration of generative AI technologies into platforms and applications.
- Played a critical role in architectural and technical review with a security mindset of critical AI initiatives like AiSera, MS Copilot, Glean AI Search, GenAI gateway, etc. to ensure responsible and secure deployment and integration into T-Mobile's environment.

Three Quality Services (Kenya - Remote) – Chief Consulting Architect (Contract). Oct 2022 – Fab 2023

Served as a chief consulting architect for different software development projects and played several roles including:

- Led the architecture design and technical review of use cases to ensure secure design, implementation, deployment, use, and maintenance.
- Led the threat modeling of different use cases to ensure inherent risk ware identified for immediate resolution.
- Collaborated with leadership to ensure the appropriate agile environment existed for agile project execution.
- Led a team of security analysts through PCI DSS assessment and audit review process.

- Led a team of developers and security analyst to use threat, vulnerability, and threat vector analysis approach to identify and implement appropriate controls to protect customer data and ensure compliance with PCI DSS.

HITRUST Alliance – Director (Research and Analysis) – Risk Management & Compliance Aug 2020 – Oct 2022

- Essential member of the management team responsible for development, promotion, and maintenance of the HITRUST Risk Management Framework (RMF) and associated tools and methodologies (Threat Catalogue, CSF, TPRM methodology, etc.).
- Ensured the updated RMF was properly mapped to all the relevant regulations/standards (e.g., NIST, ISO, GDPR, PCI, HIPAA, CCPA, etc.)
- Led a working group to develop a process for threat modeling of mobile solutions architectures and the applications of HITRUST enumerated controls to address identified risk.
- Reviewed executive order 14028: Improving the Nation's Cybersecurity and other relevant sources such as Cybersecurity and Infrastructure Security Agency's (CISA) ransomware guide and updated ransomware guidance in the HITRUST Threat Catalogue and collaborated with a group of experts to map the HITRUST CSF control specifications to the FAIR Control Analytics Model (FAIR-CAM) to enable organizations in the FAIR community to leverage the HITRUST CSF control specifications and vice versa.
- Served as a member of a supply-chain cybersecurity risk management working group that worked on the development of tools/methods to support the United State Government's supply-chain risk management efforts through a PPP arrangement.

Lindenwood University – Assistant Dean (IT/Cybersecurity) Oct 2016 – Aug 2020

- Set an IT and Cybersecurity practice center, developed courses and repeatedly taught graduate level courses on risk assessment and secure software development, which among other things covered secure architecture design, secure integration, threat and vulnerability analysis; threat modeling; identification, development, and implementation of controls; analysis of different types of controls (organizational/administrative, technical, and physical); and control functions (Loss event, Variance management, and Decision support).
- Developed, implemented, and collaborated with the Dean and other relevant departments to launched industry-driven trimester Cybersecurity and IT graduate programs for non-traditional (working) students and supervised the redevelopment and update of undergraduate cybersecurity, IT, and software development programs and led a review of IT/Cybersecurity programs to ensure they complied with accreditation policies and requirements.
- Collaborated with the IT helpdesk manager to establish a flagship internship program on campus to provide hands on experience to IT/Cybersecurity students and represented the Cybersecurity/IT department at several conferences, workshops, and meetings.

Three Quality Services (Kenya- Remote) – Co-founder *(This was allowed by Lindenwood)* Oct 2014 – Aug 2020

Served as the Lead consulting architect for different software development projects across industries (e.g., technology and finance):

- Led a team of remote security analysts to design, implement and deploy web-based applications for different clients and collaborated business teams to ensure secure deployment.
- Led the architecture design and threat modeling of different applications using different techniques such as DREAD, and STRIDE, to ensure solutions architects were free of inherent risk before implementation.
- Leveraged different frameworks (e. g., NIST CSF, NIST 800-53, FFIEC, ISO 27001/2, etc.) to analyze inherent risk and control maturity and identified residual risks for resolution.

Anritsu Company – Secure Software Development Project Manager Sept 2009 – Oct 2014

- Served as a Project Manager for the development of software test automation packages for companies such as ATT and T-Mobile and collaborated with clients and other stakeholders to ensure requirements were securely gathered, securely designed, and securely implemented.
- Very instrumental in the management and development of a team of offshore developers and test automation engineers and played a significant in the adoption of agile/scrum for software project delivery, especially by offshore teams.
- Collaborated with systems admins to harden the development environment by ensuring all servers were configured by the configuration management guidelines and all default settings were changed and ensured all development activities were conducted by the department's software development guidelines and industry best practices.

TapRoot Systems – Sr. Software Assurance and Testing Lead Mar 2007 – Sept 2009

- Actively collaborated with architects, development, and testing leads to ensure security principles were followed in each phase of the SDLC and vulnerabilities in software were identified and addressed before release.
- Ensured database servers and other systems/environments (e.g., build environment) that were critical to the development and release of software were physically protected.