

SAMUEL OWUSU

Cell: 443-653-4409 | Email: owusamuel01@gmail.com | Richmond VA 23231

AN INFORMATION SECURITY & DATA PRIVACY PRACTITIONER

A seasoned Information Security and Data Privacy practitioner with deep expertise in building enterprise privacy programs, engineering data protection solutions, and governing sensitive information across complex environments. Experience includes developing and enforcing privacy policies, conducting DPIAs/PIAs, managing DSAR workflows, and advising executives on regulatory compliance for GDPR, CCPA, HIPAA, and emerging global standards. A Data Privacy Engineer, designing and implementing privacy-by-design architectures, deploying encryption, anonymization, and identity access controls, and automating data mapping, retention, and consent processes to reduce risk and strengthen compliance. An information governance background supporting leadership in data classification, metadata management, and lifecycle controls that ensure data integrity, quality, and accountability—recognized for bridging legal, technical, and business domains to deliver secure, compliant, and privacy-preserving systems that support organizational resilience and innovation.

TECHNICAL COMPETENCIES

- Proven experience in developing and executing data governance strategies across large, complex organizations.
- Experience with regulatory compliance and data protection laws such as GDPR, CCPA, HIPAA, etc.
- Strong understanding of data management, data quality, metadata management, and data privacy principles.
- Knowledge of data management tools, platforms, and technologies (e.g., data catalogs, data quality tools, metadata management tools).
- Strong leadership, strategic thinking, and communication skills.
- Ability to work effectively with cross-functional teams and senior leadership.
- Excellent analytical skills with a deep understanding of data governance and data management practices.
- Familiarity with data architecture, cloud platforms, and modern data analytics tools.
- Expertise in risk management and regulatory compliance related to data.
- Strategic thinker with the ability to influence organizational change.
- Detail-oriented with a focus on data integrity and compliance.
- Strong problem-solving skills and the ability to navigate complex challenges.

WORK EXPERIENCE

Virginia Department of Social Services

, Richmond, VA 04/2020- Present

Sr. Data Privacy Manager

Accomplishments:

- Led the development and implementation of a GRC program that increased compliance alignment by 40% across regulatory frameworks and internal standards, reducing organizational risk exposure and enhancing security maturity.
- Established an enterprise-wide data governance framework and data stewardship model that improved data quality scores by 35% and enabled consistent metadata and classification practices across all departments.
- Led implementation of the organization's first centralized data catalog, increasing data discoverability by 60% and accelerating analytics and privacy teams' access to compliant, trusted datasets.
- Designed and deployed privacy-preserving technologies (tokenization, anonymization, encryption) across three enterprise platforms, reducing sensitive data exposure by 70% and supporting secure product launches.
- Built and operationalized a complete privacy compliance program that aligned with GDPR, CCPA, and HIPAA, reducing regulatory exposure by 40% and ensuring successful audits with zero significant findings for two consecutive years.
- Implemented new risk assessment and compliance monitoring methodologies, decreasing audit preparation time by 30% and improving visibility into enterprise risks through consistent KPI and metrics reporting.

Tasks Performed

- Develop, implement, and maintain the organization's privacy program and policies.
- Oversee processes for data subject rights requests (access, deletion, correction, portability).
- Provide ongoing privacy training and awareness programs for employees.
- Review contracts and vendor agreements for privacy risks and required data protection clauses.
- Advise leadership on privacy risks, incidents, and mitigation strategies, including breach response.
- Oversee data quality management, including data profiling, cleansing, and master data governance.

- Lead data cataloging, metadata management, and enterprise data classification efforts.
- Coordinate data stewardship roles and responsibilities across business units.
- Manage data lifecycle processes, including retention, archival, and disposal.
- Facilitate data governance councils, working groups, and cross-functional decision-making.
- Oversee data quality initiatives, ensuring data is accurate, complete, and consistent across systems and platforms.
- Establish data quality metrics, monitoring systems, and reporting mechanisms to identify and address data issues proactively.
- Lead the implementation of data cleansing and validation processes to improve data integrity.
- Collaborate with legal and compliance teams to manage data-related risks, including privacy and security risks.
- Oversee the implementation of data access controls and auditing mechanisms to prevent data misuse and breaches.
- Keep abreast of evolving data-related regulations and recommend policy and practice changes as needed.
- Partner with business leaders, IT, data scientists, and data analysts to ensure data governance practices support business needs and objectives.
- Facilitate cross-functional collaboration to ensure consistent, accurate data reporting and analytics.
- Work closely with data stewards and other operational teams to implement data governance practices across various data domains.
- Foster a culture of continuous improvement by recommending and implementing new technologies, tools, and methodologies for data governance
- Design and implement privacy-preserving technologies such as anonymization, pseudonymization, and encryption.
- Build and maintain technical controls to enforce data minimization and purpose limitation.
- Implement secure data flows, access controls, and identity management aligned with privacy requirements.
- Work with system engineers to automate privacy compliance processes (e.g., data mapping, consent management, retention workflows).
- Work with developers to embed privacy-by-design principles into new products and systems.
- Monitor systems for privacy violations, data leakage, or improper data usage.

Department of Motor Vehicles, Richmond, VA

03/2017 – 04/2020

Senior IT Auditor

Accomplishment

- *Supported over 50 risk assessment and IT audit projects, identifying critical vulnerabilities, threats, and risks and implementing strategic mitigations that decreased risk exposure by over 30% across various platforms and technologies.*

Tasks Performed

- Conducted internal audits and assessments to evaluate the effectiveness of compliance controls
- Led and participated in multiple compliance audit engagements that led to certifications.
- Monitored compliance with applicable security policies and reported related risk issues to management.
- communicated the audit assurance program of systems managed by vendors.
- Identified and appropriately communicated audit issues to management, offering recommended solutions that addressed risks and were relevant to the business.
- Reviewed and assessed the risk of cloud service providers and conducted and maintained vendor risk assessments.
- Provided timely updates to team members and audit management on engagement progress and audit issues, ensuring all deadlines were consistently met.
- Briefed senior leaders and executives on the threat landscape and the organization's risk profile and recommended a Security Strategy.
- Support and coordinate external audit engagements

Baltimore City Community College: Baltimore, MD

02/2015- 03/2017

Information Security Risk Specialist:

Accomplishment

- Executed a comprehensive application security strategy, incorporating secure coding practices, automated vulnerability scans, and continuous monitoring. This resulted in a 30% reduction in critical vulnerabilities across all major applications and was pivotal in achieving compliance with stringent industry standards, notably OWASP Top 10

Tasks Performed

Risk & Vulnerability Management

- Coordinated and communicated with stakeholders to plan and ensure corrective actions are implemented to address identified vulnerabilities.
- Performed comprehensive analysis of vulnerabilities and reports to help develop and implement appropriate remediation strategies.
- Evaluated vulnerabilities of third-party applications and reported compliance based on prioritization criteria.
- Investigated and conducted root cause analysis on persistent or recurring vulnerabilities.

- Served as a primary point of contact and supported the business units in addressing concerns, issues, and escalations related to vulnerability findings and remediation plans.
- Developed and implemented information security and risk management programs.
- Performed quantitative and qualitative risk assessments, ensuring actions were taken to mitigate them.
- Communicated results of vulnerability and risk assessments to system and data owners

Support Analyst (Part-time) Kohl's Departmental Store Edgewood, MD

09/2013- 02/2015

- Supported Cloud and non-cloud privacy programs and due diligence programs.
- Created schedules to perform annual security assessments of sensitive systems.
- Developed security policies and ensured their continuous update.
- Supported the implementation and administration of privacy management technology.

EDUCATION

- | | |
|---|---------------------------------|
| • Marymount University
DSc. Cybersecurity | Arlington, VA
May, 2023 |
| • University of Maryland, Baltimore County (UMBC),
M.Sc. in Information Systems, | Baltimore, MD
December 2013. |
| • University of Education,
Bachelor of Education, | Winneba, Ghana,
June 2005 |

CERTIFICATIONS

- **CISSP – Certified Information Systems Security Professional**
- **CISM – Certified Information Security Manager**
- **CISA – Certified Information Systems Auditor**
- **CIPT – Certified Information Privacy Technologist**
- **Sec+ – CompTIA Security+**