THOMAS W. ANOKYE

Melissa, TX | (972) 358-1389 | t.anokye7@gmail.com | www.linkedin.com/in/thomas-w-anokye

PRINCIPAL SENIOR SECURITY ANALYST – IT SECURITY & COMPLIANCE
Information Systems Risk Management | Governance & Risk Compliance | Cybersecurity Audit

PROFESSIONAL SUMMARY

With a bachelor's degree in information systems and cyber security and over 10 years of technical experience in information security and privacy, I am a seasoned professional in the field. Holding multiple certifications, including CISM, CRISC, and CISA, I am committed to maintaining current knowledge. My expertise spans regulatory compliance, risk assessment, and threat analysis across various domains, such as finance, IT, information security, and privacy. Proficient in GRC frameworks like HITRUST, NIST, ISO, COBIT, and ITIL, I excel at identifying vulnerabilities and leading cross-functional teams. I possess strong communication skills, delivering concise reports and presentations. My leadership in the industry is underpinned by proven experience with a focus on achieving robust security and compliance standards.

IT Compliance Program |Information Systems |IT General Controls |IT SOX Audits |GRC Governance & Risk Compliance | Identity & Access Management | Cyber Security Audit | Incident Management & Response |Vulnerability Assessment |SOX | Key metrics | CRMA |Computer Science |Work Independently |Operating Procedures| Analysis of Business| Team Management | Technical Knowledge |Regulatory Compliance | Risk Mitigation |AWS | Excellent writing skills | Performance Analysis | Scrum | Enterprise Risk | Identifying risks |Pragmatic | SAAS | IT Risk Management | Technical Knowledge | Security Analysis | Accuracy | GRC |SOC | DNS| IT Audit | Internal Controls | Internal Audit | Relationship Building |Project Leadership | Security Assessments | Articulate | SIEM | OWASP |Dynatrace | Problem-Solving | Vulnerability Management | Project management | Analytics | Cloud Security | Agile | Azure | GDPR

WORK EXPERIENCE

Medtronic – Remote, TX • 04/2025 – Present
Principal Security Compliance/Third-Party Risk Management Analyst

- Developed and implemented enterprise AI Governance policies, standards, and procedures to establish responsible AI usage, risk management, and regulatory compliance requirements.
- Authored AI governance documentation covering acceptable use, data protection, privacy, security controls, human oversight, model accountability, and ethical AI best practices.
- Established governance frameworks and control requirements for the evaluation, approval, deployment, and ongoing monitoring of AI-enabled technologies and third-party AI solutions.
- Conducted AI risk assessments to identify cybersecurity, privacy, compliance, operational, and reputational risks associated with AI adoption.
- Collaborated with Legal, Privacy, Security, and business stakeholders to define AI governance requirements aligned with organizational risk tolerance and regulatory obligations.
- Developed procedures for reviewing and approving AI tools, including requirements for vendor due diligence, data classification, sensitive data protection, and security control validation.
- Defined controls and guidance to prevent the unauthorized use of AI technologies and the exposure of confidential, regulated, or proprietary information.

- Advised leadership on emerging AI regulatory requirements, industry best practices, and governance considerations to support responsible AI adoption.
- Integrated AI governance requirements into existing risk management, third-party risk management, and compliance programs.
- Led awareness and training initiatives to educate employees on AI governance requirements, acceptable use expectations, and responsible AI practices.
- Lead and managed end-to-end third-party cybersecurity risk assessments, including scoping, evidence review, control evaluation, and risk rating in alignment with Medtronic's enterprise risk program.
- Review and validate VRAs (Vendor Risk Assessments) completed by other analysts to ensure accuracy, completeness, and alignment with internal quality standards.
- Developed standardized risk assessment documentation and guidance materials, enabling consistent execution of third-party risk evaluations across analysts and stakeholders
- Identify, document, and communicate security/privacy risks, control gaps, and required remediation actions, ensuring clear recommendations for risk-based decision making.
- Collaborate closely with internal stakeholders, including Legal, Procurement, Privacy, and Security Engineering, to drive remediation and ensure risks are understood and addressed.
- Support the continuous improvement of third-party risk assessment workflows, documentation standards, and intake processes.
- Serve as a key stakeholder on the LogicGate and OneTrust GRC system implementation projects, providing feedback on workflow design, requirements, and future-state processes.
- Perform UAT (User Acceptance Testing) for LogicGate and OneTrust, validating functionality, testing new workflows, and identifying system defects or enhancement opportunities.
- Partner with cross-functional teams to operationalize new GRC processes, improving efficiency and consistency across TPRM operations.
- Facilitate vendor remediation by tracking corrective actions, validating evidence, and ensuring issues are resolved within expected timelines.
- Contribute to policy, standard, and procedure updates related to third-party cybersecurity, privacy, AI risk considerations, and vendor lifecycle governance.
- Provide clear, concise reporting on assessment outcomes, key risks, and vendor posture to leadership and downstream teams.
- Process security and privacy intake forms in ServiceNow, ensuring completeness, proper routing, and initiation of VRA and privacy assessments.
- Manage and triage procurement-related ServiceNow tickets, confirming vendors follow required security, privacy, and sourcing workflows prior to onboarding or purchase.
- Designed and contributed to the standardization of enterprise risk register artifacts, including risk taxonomy, classification structures, and consistent documentation of vendor and technology risks
- Applied a risk scoring and prioritization model leveraging likelihood and impact criteria, ensuring consistent risk rating and escalation across third-party assessments
- Supported the risk governance lifecycle, including intake, assessment, risk acceptance, and continuous monitoring workflows within ServiceNow and LogicGate.

CVS/Aetna – Remote, TX

SR. Security Risk Compliance Analyst - Third Party Risk Management • 04/2024 – 04/2025

- Lead comprehensive security risk assessments at enterprise, organizational, and technology levels, identify vulnerabilities, enforce compliance standards, and ensuring robust protection against potential security threats during TPRM reviews.

- Conduct in-depth security evaluations of key vendors and business partners, implementing rigorous security standards to safeguard corporate data and infrastructure.
- Provide expert security consultation for IT and business projects, influencing project outcomes with strategic risk management and advanced security solutions.
- Delivered a complete risk management framework, including risk register design, scoring model, governance workflows, and documentation, enabling a scalable and repeatable enterprise risk program
- Authored comprehensive risk management documentation, including risk register standards, scoring methodologies, and governance procedures for enterprise use
- Led knowledge transfer initiatives, providing guidance and documentation to stakeholders to ensure consistent adoption of risk management practices
- Develop, enhance, and maintain the organizational security risk framework and risk register using Archer, ensuring strategic alignment with business objectives and IT strategies.
- Coordinate and lead third-party security assurance activities, managing intricate security requests and overseeing comprehensive compliance-driven tasks.
- Oversee the creation, implementation, and maintenance of security policies and standards, managing policy exceptions and adapting policies to evolving security landscapes and regulatory requirements.
- Design, develop, and deliver targeted security training and awareness programs, significantly enhancing the security knowledge base and culture within the organization.
- Generate detailed security risk reports and develop robust key risk indicators (KRIs), key performance indicators (KPIs), and dashboards, providing actionable insights and decision-support tools to senior management.
- Facilitate cross-departmental collaboration to integrate security practices into business processes, enhancing operational efficiency and security posture.
- Proactively monitor and manage security incidents and breaches through a refined security ticketing system, reducing response times and mitigating potential impacts.
- Recommend and implement technical controls, encryption mechanisms, access controls, and data safeguards to protect classified data from unauthorized access, disclosure, or misuse.
- Developed and maintained the enterprise risk register framework within RSA Archer GRC platform, including standardized templates, risk taxonomy, and reporting structures
- Designed and implemented a risk scoring methodology with defined likelihood and impact scales, enabling consistent prioritization of enterprise and third-party risks
- Built risk prioritization models and heat maps, supporting executive-level decision making and remediation planning
- Developed DLP policies and procedures to adhere to regulatory compliance and reduce risk to the organization.
- Adhere to controls and requirements of frameworks such as HITRUST, NIST, IS27001, COBIT 5.

CAPIO – Sherman, TX

Security Risk Compliance Manager • 07/2020 – 04/2024

- Conducted regular risk assessment and control audits, strengthening the overall security posture of the organization. Performed risk assessment over tools run in the AWS Cloud platform to ensure it was structured in a way to align IT with business goals while managing risks and meeting all industry and government regulations.
- Headed the TPRM Initiative, performing IT audits and Gap / Risk assessments of current and potential vendor relationships.
- Produced formal documentation packages and operational procedures for risk management, supporting ongoing governance, audits, and program scalability

- Executed comprehensive SOC assessments and evaluations of external vendors and agencies as an integral component of the Third-Party Risk Management (TPRM) process.
- Actively contributed and oversaw annual HITRUST assessments by providing thorough documentation of current CSF controls.
- Executed meticulous risk assessments over the HIPAA Environment, vital in maintaining Capio's PCI and HITRUST certifications.
- Mapped security controls and requirement statements to policies and procedures, aligning with the HITRUST and NIST CSF revalidation process.
- Established information security policy standards, procedures, and guidelines, aligning with relevant regulations and industry best practices.
- Championed information security program initiatives, coordinating with various lines of business and assisting in the implementation of comprehensive safeguards.
- Led the Security Incident Response team, coordinating effective incident responses, reporting, and learning documentation.
- Conducted tabletop exercises and mock incidents to rigorously test the Incident Response Plan and Disaster Recovery.
- Fostered a robust security culture within Capio by organizing security awareness campaigns and training sessions, including the creation of security training content to help strengthen the overall GRC program.
- Performed detailed security audits and event investigations, adhering to forensic guidelines to preserve potential evidence for legal proceedings.
- Authored comprehensive policies and procedures for Capio, encapsulating HITRUST controls and relevant requirements.
- Oversaw the enforcement of Capio's contract management system as part of the TPRM program.
- Managed diverse information security projects, including the implementation of new technologies and the enhancement of existing GRC tools.
- Led the initial population of risk registers across HIPAA and PCI environments, ensuring visibility into key cybersecurity and compliance risks
- Authored risk management procedures and operational documentation, supporting long-term sustainability of the GRC program
- Coordinated information security and awareness training programs, conducting phishing campaigns, and delivering weekly training through a learning management system.
- Researched emerging threats, evaluated their likelihood of occurrence, and designed controls to mitigate them.
- Identified vulnerabilities within the Capio environment, overseeing associated remediation activities.
- Devised and executed tests for security implementation and adherence to security practices.
- Responded to security questionnaires from Capio customers, detailing the robust measures in place to protect health information.

FRONTIER COMMUNICATIONS – Allen, TX
SR. IT Security Analyst - 07/2019 – 07/2020

- Directed and oversaw assessment, selection, implementation, and maintenance of information security tools & technologies and frameworks such as ITIL, COBIT, NIST, and ISO/27002.
- Participated in business continuity planning (BCP) activities required by senior leadership. Enforced information security controls and investigated/responded to security incidents.
- Conducted comprehensive security assessments across the organization's IT infrastructure, identifying vulnerabilities and potential threats.
- Created security policies and procedures aligned with industry standards and regulatory requirements.
- Served as a subject matter expert, providing guidance on security best practices and compliance to internal teams.

- Conducted vulnerability assessments, pinpointing weaknesses in systems and applications.
- Evaluated and recommended enhancements to incident response and disaster recovery plans.
- Coordinated with external auditors, facilitating security audits and compliance assessments.
- Proactively monitored security alerts and swiftly responded to security incidents, ensuring timely resolution.
- Developed and delivered comprehensive security training programs for employees, promoting awareness and adherence to security protocols.
- Developed and applied risk scoring methodologies using likelihood and impact scales, enabling structured prioritization of vulnerabilities, third-party risks, and security gaps across enterprise systems
- Oversaw the development and upkeep of security documentation, including policies, procedures, and incident reports.
- Collaborated with legal and compliance teams to address data privacy and regulatory compliance requirements.
- Leveraged the Archer Governance, Risk Management, and Compliance (GRC) platform to automate and streamline risk assessments, ensuring comprehensive coverage.
- Implemented security controls and maintained compliance with regulatory standards, including PCI DSS, utilizing Archer for tracking and reporting.
- Integrated Zycus, a contract management solution, into the TPRM process, ensuring secure and compliant vendor relationships.
- Conducted thorough assessments of third-party vendors through Zycus, evaluating their security controls and contractual adherence for TPRM review.
- Coordinated with legal teams to review and negotiate security-related vendor contract clauses, optimizing contract management through Zycus.
- Maintained comprehensive documentation within Archer, encompassing risk assessment reports, control implementation plans, and compliance dashboards.
- Aligned IT service management processes with security best practices, following the ITIL framework.
- Analyzed security data from various sources, including SIEM solutions, proactively identifying security incidents and vulnerabilities.
- Delivered regular security training sessions to employees, emphasizing the significance of security and compliance.
- Supported the development and maintenance of risk registers within RSA Archer GRC platform, documenting and tracking enterprise security risks and mitigation efforts
- Applied risk scoring methodologies using likelihood and impact criteria, enabling structured prioritization of identified vulnerabilities and threats.

HKS ARCHITECTS – Dallas, TX

Security Analyst • 04/2016 – 07/2019

- Lead information security and awareness training initiatives, overseeing phishing simulations, and administered training sessions via a learning management system.
- Resolved associated IT compliance gaps by applying effective information assurance procedures and policies, including change management security policies, disaster recovery, release management, and systems maintenance.
- Acted as an end-to-end expert in managing IT-related initiatives, effectively achieving and sustaining compliance with regulatory, industry, and contractual terms.
- Supported the development of risk scoring and prioritization frameworks, incorporating likelihood and impact criteria to assess and rank organizational risks
- Resolved IT compliance issues and performing root cause analyses on all escalated risks, thus optimizing all organizational software and computer programs.
- Enforced security protocols to protect company information from unauthorized access, modification, and destruction.

- Implemented GRC best practices by creating SOPs and DLP and training all staff members on mitigating evolving security risks, increasing security awareness within the company.
- Conducted risk assessments to identify potential vulnerabilities and threats across the organization's systems and processes.
- Collaborated with various departments to develop and implement governance policies and procedures, ensuring alignment with industry standards and regulations.
- Assisted in the development and maintenance of the organization's risk management framework.
- Monitored compliance with internal policies, industry regulations, and external standards.
- Conducted regular audits and assessments to evaluate the effectiveness of control measures and compliance efforts.
- Provided guidance and training to internal teams on compliance best practices and policies.
- Utilized GRC software tools and platforms to streamline risk assessment, compliance tracking, and reporting processes.
- Prepared and presented comprehensive reports and dashboards on risk and compliance status to senior management.
- Played a key role in incident response and data breach investigations, ensuring compliance with data protection regulations.
- Assisted in the development of business continuity and disaster recovery plans, ensuring they align with compliance requirements.
- Assisted in the development of risk management frameworks and risk register documentation, supporting structured identification, assessment, and tracking of organizational risks
- Conducted vendor risk assessments to evaluate the security and compliance practices of third-party suppliers.
- Collaborated with legal teams to address data privacy and regulatory compliance requirements.
- Stayed up to date with industry trends and changes in regulations to ensure the organization's ongoing compliance efforts.
- Contributed to the development and execution of security policies and procedures to align with industry standards and regulatory mandates.

CAPITAL ONE CORPORATE OFFICE – Plano, TX
Field Service Engineer • 11/2013 – 04/2016

- Steered successful migration of users from Windows XP to Windows 7 while ensuring business continuity throughout the organization.
- Troubleshot all software and hardware-related issues and deployed equipment to laptop users.
- Developed Good Mobile Enterprise and Air Watch for Android, iPhone, and Blackberry users.
- Delivered top-tier customer service by promptly resolving tickets and work orders within SLA using the HP Service Manager ticketing system as per the support desk SOPs.
- Installed, repaired, and sourced network equipment, ensuring seamless network connectivity within the company and business continuity.

GWA INNOVATIVE TECHNOLOGY, INC. – Richardson, TX
Jr. Network Administrator • 11/2010 – 11/2013

- Maintained uninterrupted network security and flow by designing telecommunication networks and systems and optimizing all hardware, software, and communication tools.
- Implemented and tested disaster recovery solutions by upgrading firewall, antivirus, and intrusion detection systems, improving security resilience.

- Configured and deployed computer gadgets after company-wide upgrade to ensure seamless network connectivity.
- Addressed network security issues and prevented unauthorized access to the systems. Analyzed end-user problems and resolved them amicably.

EDUCATION

Bachelor of Science: Information Systems and Cyber Security (ISC)
ITT Technical Institute – Richardson, TX
2012 – 2014

Associate degree: Information Technology & Computer Network Systems (CNS)
ITT Technical Institute – Richardson, TX
2010 – 2012

CERTIFICATIONS

Certified Governance of Enterprise IT (CGEIT)| ISACA, Pursuing
Certified in Risk and Information Systems Control (CRISC) | ISACA, Jun 2021 - Success
Certified Information Systems Auditor (CISA) | ISACA, Mar 2021 - Success
Certified Information Security Manager (CISM) | ISACA, Feb 2021 - Success
Certified information systems security professional (CISSP) | Pursuing