Richard

Bronx, NY

**Email:** **nishant@stglobaltech.com**

 **Contact: 513-286-7784**

Results driven leader with over 10+ years of experience. Extensive knowledge in Cybersecurity and Information Security management activities with focus on Risk Management and compliance activities. Experience using Industry Risk Management Frameworks to Improve organizations cybersecurity.

Holds an Active Secret Clearance.

# Work Experience

## Information System Security Specialist

NYC Board of Elections - Bronx, NY January 2017 to Present

* Collaborating with Business/LOB Risk partners (Control Owners, Performance Managers, Application System Managers etc..) to perform validation testing for assigned controls, testing the operating and design effectiveness of technology controls through gathering evidence, analyzing and documenting test conclusions including identifying issues in the event of control failures.
* Work with IT QA Testing team to gather evidence, develop test plans, testing procedures, updating testing guidance documents and document test results and exceptions.
* Participate in the SOX testing of the IT General Computer Controls.
* Conduct ITGC control testing including reviewing the effectiveness and efficiency of Operational and Information Technology procedures and providing recommendations on their adequacy, accuracy and compliance with organizational policy.
* Assists in the execution of the Line of Business Risk Management program, identifying opportunities for enhancement where applicable. Under supervision, enables line of business adherence with risk programs.
* Assists in the design and development of the risk management program to meet business and regulatory expectations.
* Executes the risk management program within or across the lines of business (e.g. – business self- assessment and quality reviews). Participates in the consultation to execute the program components.
* Works to develop risk expertise while working with the businesses and other risk partners (e.g., Compliance, Credit, Legal, Audit).
* Participates in risk initiatives, business as usual activities, ad hoc requests, and identifies risk exposures
* Plays integral role in Scanning software for security issues and provide manual reviews
* Collaborates with developers on the team to ensure success
* Discovers vulnerabilities and provide results for prevention
* Reviewed authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.
* Verified that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations.
* Collaborate on information security related incidents and resolution with technical staff, and provide security expertise/knowledge to cross functional information management teams.
* Conducts audits of the security levels, security practices and provides updated status reports.
* Participates in the security incident response team, including performing forensics analysis, and documentation.
* Interviews and investigations to mitigate future vulnerabilities.
* Responsible for virus/malware removal and identifying and implementing preventative controls and measures.

## Information System Security Specialist

UNITED STATES DEPARTMENT OF COMMERCE - U.S. CENSUS BUREAU - Bronx, NY

August 2013 to December 2016

* Initiate meetings with various System Owners and Information System Security Officers (ISSO), providing guidance and evidence needed for security controls, and documenting findings of assessment.
* As a team, we determine Security Categorizations using FIPS 199 as a guide, review, update, and develop Privacy Impact Assessment (PIA), Privacy Threshold Analysis (PTA), and initiate System Security Plans (SSP).
* Update System Security Plans (SSP) Using NIST 800-18 as a guide; assess Incident Response Plans; create Change Control procedures and drafts; and review updates on Plan of Action and Milestones (POA&Ms).
* POA&M Remediation: Perform evaluation of policies and procedures, security scan results, and system settings in order to address controls that were deemed insufficient during Certification and Accreditation (C&A).
* Expertise in National Institute of Standards and Technology Special Publication (NIST SP) documentation: Perform assessments, assist with POA&M creation and remediation, using NIST SP 800-53 Rev.1 and NIST SP 800-53 rev.4.
* Develop solutions to security weaknesses in the Requirement Traceable Matrix (RTM) and SAR, while working on POA&M remediation and Corrective Action Plan (CAP).
* Review updates on System Security Plan (SSP) using NIST SP 800-18 guidelines.
* Specialize in the entire FISMA Risk Management Framework (RMF), and system control assessment processes using NIST SP 800-60, NIST SP 800-53A, preparing and reporting on SSP, SAP, PTA, PIA, E- Authentication ST&E, and POA&M.
* Develop and conduct ST&E (Security Test and Evaluation) according to NIST SP 800-53A, perform on- site security testing and review vulnerability scan results.
* Effectively communicate with multiple clients to perform POA&M remediation, also handle internal communications within the Office of Information Security and external communications with several different divisions daily. Maintain excellent working relationships with both internal and external clients using good communication skills.
* Provide security control assessor (SCA) services, such as assisting with the Assessment and Authorization process, including A&A scanning, documentation, reporting and analysis – analyzing current threats to information security and systems.
* Collaborate with external vendors, consultants, and other third parties to improve information security within the organization.
* Identifies attacks to the Health System network and systems and escalates security issues to facilitate prompt remediation.
* Identifies, tracks, and monitors information security threats to support service continuity and security management.
* Contributes on implementation of and testing of disaster recovery plans.
* Participates in performing risk assessments for new business relationships/partnerships, software, and protected data/assets.
* Lead information security projects such as, security architecture, endpoint protection,

anti-virus/anti-malware, server hardening, encryption, patching, firewall configurations and log management.

* Keep current with security threats, new privacy and security legislation, and security technologies.
* Perform other duties as assigned.

## Information System Security Specialist

Bankers Life - Bronx, NY

April 2010 to December 2012

* Performed security reviews, identified gaps in security architecture, and developed a security risk management plan.
* Performed risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.
* Provided input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).
* Ensured that security design and cybersecurity development activities are properly documented (providing a functional description of security implementation) and updated as necessary.
* Supported necessary compliance activities (e.g., ensure that system security configuration guidelines are followed, compliance monitoring occurs).
* Assist with the Risk Management Framework (RMF) process using NIST SP 800-37 as a guide for assessments and Continuous Monitoring.
* Validate system security requirement definition and analysis, and review System Security Plans for enterprise-wide architectures.
* Perform Security Risk Assessment and risk analysis of resources, controls, vulnerabilities, impact of losing systems’ capabilities, and threats to the mission objective.
* Perform analysis to facilitate decisions to implement security countermeasures or mitigate risks; assist with the implementation of countermeasures.
* Periodically review programs, recognize possible threats, and review evaluations for compliance and non-compliance.
* Provide guidance on vulnerability and malware remediation.
* Draft/create/review RMF documents such as Configuration Management Plan, Incident Response Plan, Contingency Plan, Security Plans and POA&Ms.
* Report generating tool for link up time, downtown and bandwidth utilization, and latency.
* Pro-active health check-up of the network and taking action plans accordingly.
* Communicating with the client for assisting in network design related to link termination.
* Maintaining the tracker for all above activities till execution.
* Coordinate and perform information security risk assessments and audits to ensure that information.
* Ensure implementation of best practices configuration and administration of information security controls and tools; e.g. access controls, endpoint protection, anti-virus/malware, data loss prevention, email security, encryption, patching, vulnerability, web application gateways, perimeter firewalls and security log management and monitoring tools, used in governance, risk management, and compliance of protected data.
* Mitigate security event alerts and vulnerabilities through security incident event management (SIEM) tools or other external sources.
* Develop and maintain technical documentation used for information security operations procedures, which outline decision support (e.g., security control administration, best practices, events of interest and incident handling, and escalation).
* Participate in information security awareness and training initiatives to educate the workforce about information risks.

# Education

## Bachelor of Science in Gerontological Studies and Services

York College / City University of New York - Jamaica, NY June 2018

## Associate of Arts in Liberal Arts

Bronx Community College / City University of New York - Bronx, NY January 2011

# Skills

* IT Controls – Frameworks: IT Audit Standards: Confidentiality, Integrity, Availability, Access Control, Audit and Accountability, Certification and Accreditation, Risk Assessment, OMB Circular A-130 Appendix III, NIST 800-53,NIST 800-53A, NIST 800-30, NIST 800-37, NIST 800-34, NIST 800-18, FIPS, FISMA, FedRAMP, SaaS, PaaS, IaaS, NIST RMF framework-DSS and HIPAA, Cisco Routers – 1841, 2611, 2620 series, Cisco Switches-3500, 3750 series, Cisco Internetwork Operating System (IOS), OSI and TCP/IP models, TCP and UDP protocols, Access point, three-tier architecture, Network topologies Star, Mesh, Hybrid. EMASS, CSAM, RISKVISION (10+ years)
* Information Security
* Cybersecurity
* Network Firewalls
* Disaster Recovery
* Network Security
* Splunk
* Active Directory
* Program management
* Security Analysis
* Authentication
* Incident Response
* Encryption
* DHCP
* Linux
* System Administration

# Languages

* English - Expert
* Asanti Twi - Expert
* Fante - Expert

# Certifications and Licenses

## Certified Information Systems Auditor (CISA)

June 2021 to January 2025

## Certified CompTIA Security + CE

March 2021 to March 2024

## Certified Ethical Hacker Certification- CEH

March 2021 to March 2024

## Scrum Master Accredited Certification

Present

# Assessments

## Project timeline management — Completed

June 2018

Measures a candidate's ability to prioritize and allocate time to effectively achieve project deliverables. Full results: [Completed](https://share.indeedassessments.com/attempts/3bc80068caad75317c2d41234886320ceed53dc074545cb7)

Indeed Assessments provides skills tests that are not indicative of a license or certification, or continued development in any professional field.