ALI H. NAQVI

Phone: (516) 413-9952 | **Email:** anaqvi1694@gmail.com | **Address:** 205 Bay Ave, Hicksville NY 11801

PERSONAL INTRODUCTION

Information security practitioner with progressive history working in the financial services and technology industry. Results-driven team player with a broad background in information technology security, risk, and audit. A creative, analytical, and detail oriented problem solver with experience driving procedure and process developments, risk assessments, security awareness, audit management, and security monitoring.

EDUCATION

CUNY John Jay College: ***M.S in Digital Forensics & Cybersecurity*** **Received July 2022**

CUNY Baruch College Zicklin School of Business: ***B.B.A in Accounting & CIS*** **Received May 2019**

WORK EXPERIENCE

BLACKROCK INC. **June 2022 – December 2022**

Information Technology Audit Associate ***New York, NY***

- Planned and executed audits of IT general controls, cybersecurity principles, compliance with key regulations and compliance frameworks, as well as technology processes across internal and customer-facing technologies to drive an improved organizational risk posture.
- Identified and tested key controls for various technology functions including system build, infrastructure resiliency, logical access, change management, information security, data classification, encryption, production monitoring, inventory management, and disaster recovery.
- Performed design and operating effectiveness testing and prepared audit work papers in accordance with approved internal guidelines.
- Documented and reported qualitative and quantitative risk assessments for inherent, detective, and control risks to Senior Management.
- Confirmed successful and timely implementation of remediation plans due to prior audit observations as part of the risk mitigation strategy.
- Created detailed flowcharts illustrating end to end business processes integrated with control mappings to identify gaps and high risk areas.
- Reviewed vendor due diligence tasks such as SLA performance metrics, patch management, external audits, and security assessments.
- Analyzed internal application and infrastructure vulnerability reports for critical and high security issues and related remediation plans.
- Maintained communication channels with stakeholders to facilitate walkthroughs, evidence requests, status updates, and issue disclosures.

SS&C TECHNNOLOGIES INC. **November 2017 – April 2021**

Information Technology Audit Associate ***New York, NY***

- Coordinated and delegated security assurance activities to multiple subordinates; tasks involved identification and gathering of evidence to verify compliance against security baselines for several business applications, operating systems, database servers, and infrastructure.
- Supported Internal Audit Management initiatives to develop effective and consistent test plans by standardizing control testing methodology, test steps, and verbiage across all auditable units to align control structure, streamline requests, and improve testing efforts.
- Routinely presented technical audit reports to Management using clear and simple terminology summarizing the broader context and implications (e.g., financial, legal, reputational, etc.) of the various types of risks affecting the business and critical technology functions.
- Partnered with cross functional departments to support corporate control objectives and strengthen relationships for better collaboration.
- Utilized excel analytics to standardize datasets and created custom scripts for automated analysis, reducing manual efforts to achieve full population testing, resulting in comprehensive and complete audit conclusions while pinpointing key risks areas and control gaps.
- Consolidated audit data and built custom dashboards to summarize internal audit team KPIs for planning and performance optimization.
- Acted as liaison between Management and External Auditors to facilitate Stakeholder expectations and ensure timely delivery of artifacts.
- Examined application developments following the Agile methodology to ensure proper completion of development activities, user stories, acceptance criteria, automated code testing, vulnerability scans, business process documents, and Management review and approvals.
- Verified corporate policies such as SDLC, BCP/DR, DLP, IAM, data classification, and user training against industry best practices.
- Investigated security incidents for root cause analysis and timely coordinated corrective action plans with Remediation Champions.

SECURITY PROJECTS

- Network Forensics: Analyzed network traffic with Wireshark to detect brute force attempts, identify flooding attacks, and review web traffic.
- Digital Forensics: Investigated device images (system registry, event logs, directories, media, etc.) to uncover evidence of suspicious activity.
- Tenable Nessus: Performed security scans to identify vulnerabilities, policy and configuration violations, and IOC on multiple assets.

SKILLS

CompTIA Security+	Microsoft VBA	ServiceNow & Jira	IDS/IPS	Zero Trust & OWASP	Intro to Python
CompTIA Network+	Azure DevOps	Splunk & Archer	Tableau	NIST, CIS, & ISO27K	SQL & DBMS
IT Risk Assurance	Data Visualization	Linux & Windows	Nessus	GDPR & SOX404	HTML & CSS