ALI H. NAQVI

Phone: (516) 413-9952 | **Email:** ali.naqvi@jjay.cuny.edu

PERSONAL INTRODUCTION

A recent M.S cybersecurity graduate with five years of demonstrated progressive experience working in information technology risk, audit, and security with high aspirations to carry out an impactful career in cybersecurity. A self-starter striving to expand his range of skills with the tools, knowledge, and training necessary to help protect an organization's cyber landscape and digital assets in a hyper connected economy.

CYBERSECURITY SKILLS

- CompTIA Security+
- CompTIA Network+
- TryHackMe Badges
- IT Risk Assurance
- ITGC Controls
- Digital Forensics
- Incident Response
- TCP/IP Stack
- Linux & Windows
- Microsoft Azure
- Palo Alto Networks
- Nessus Essentials
- ServiceNow & Jira
- VirusTotal
- CrowdStrike Falcon
- Wireshark
- Autopsy
- Splunk
- Tableau
- Archer
- Zero Trust Security
- NIST SP 800 & CSF
- GDPR & SOX404
- MITRE ATT&CK
- FFIEC IT Handbook
- Microsoft VBA
- SQL & DBMS
- HTML & CSS
- Intro to C++
- Intro to Python

RELEVANT WORK EXPERIENCE

BLACKROCK **June 2022 – Present**

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

- Co-lead risk based audits to identify, test, and report on technology dependent controls including system build and resiliency, change management, information security, capacity and performance, production monitoring, identity and access, and inventory management.
- Execute design and operating effectiveness assessments to evaluate control performance against corporate policies and industry standards.
- Maintain communication channels with stakeholders to facilitate walkthroughs, evidence requests, status updates, and issue escalations.
- Create detailed flowcharts illustrating end to end business processes integrated with control mappings to identify gaps and high risk areas.
- Perform action verifications for prior audit findings to confirm successful implementation of recommended action plans for risk mitigation
- Review 3rd party vendor due diligence tasks to verify performance metrics, SOC Report reviews, and info-sec assessments were conducted.

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

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

- Hired as an Intern and progressed to Sr. Associate within 3 years due to continuously exceeding management's performance expectations.
- Routinely presented technical audit reports and KPIs to Senior Management, using clear and simple terminology, summarizing progress towards audit deliverables, communicating areas of concern, and providing feasible recommendations for operational improvements.
- Supported Internal Audit Management initiatives to develop effective and consistent test plans by standardizing control testing methodologies and verbiage across all auditable units to align control structure, streamline requests, and improve testing efforts by 50%.
- Utilized excel analytics to standardize system reports and created custom scripts for systematic analysis, reducing manual efforts to achieve 100% 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 IA team KPIs for planning and performance optimization.
- Investigated security incidents for root cause analysis and timely coordinated corrective action plans with remediation champions.
- Acted as a liaison between Management and external auditors to facilitate requirements and timely delivery of audit artifacts.
- Participated in ongoing training efforts to improve audit skills and remain up-to-date with relevant industry regulations and standards.

CYBERSECURITY 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 including file systems, logs, messages, media, and GPS to uncover evidence of criminal activity.
- Tenable Nessus: Performed custom scans to identify known vulnerabilities using host enumeration, port scanning, and service discovery.
- Palo Alto NGFW: Configured and deployed a firewall to monitor App ID, User ID, and Content ID for possible indicators of compromise.
- MITRE: Utilized ATT&CK Navigator to perform a risk and gap analysis by mapping capabilities and prioritizing investment opportunities.

GRADUATE & UNDERGRADUATE EDUCATION

M.S IN DIGITAL FORENSICS AND CYBERSECURITY **Received July 31, 2022**

John Jay College of Criminal Justice (GPA: 4.00) ***New York, NY***

B.B.A IN ACCOUNTING WITH MINOR IN COMPUTER INFORMATION SYSTEMS **Received May 2019**

Bernard Baruch College, Zicklin School of Business (GPA: 3.5) ***New York, NY***