**Muhammad Aamir Khan**

**Lead Cyber Security and Information Security Architect**

[**https://www.linkedin.com/in/aamir-khan-mscs-mba-ccnps-cfcp-cism-crisc-cisa-mcse-60892916a/**](https://www.linkedin.com/in/aamir-khan-mscs-mba-ccnps-cfcp-cism-crisc-cisa-mcse-60892916a/)

**347 667 4667**

[**muhammad.aamir2351@gmail.com**](mailto:muhammad.aamir2351@gmail.com)

**NYC, NY**

**TN Visa || C2C Only**

**Ready to go onsite from Day in anywhere in USA.**

**Professional Career Profile:**

**15 + years of Extensive Professional Experience in Cyber Security Project / Program management and Cyber Security Trainings Cyber Security / Network Security / Information Security / College Teaching in 6 Countries Worldwide**

**Professional Skills**

* Cyber Security Design, Operations and Management
* Cyber security Incident and Offensive Management
* Cyber Security Disaster / Continuity Management
* Cyber Security Threat Intelligence
* Cyber Security Professional Trainings and Awareness
* Cyber Security Project, Program and Change Management
* Cyber Security Audit
* Application security / Vulnerability Management
* Cloud Security, Routers, Switches, Firewalls, Endpoints Protection
* CISO Management
* **GRC**
* Information Security Policies, Controls, Governance and Compliance
* NIST, ISO, MITRE ATTACK, PCI DSS,SABSA and TOGAF
* SIEM (Security Event and information Management)
* IOT (Internet of Things)
* College Teaching, specialized in Cyber Security / Information Security Domain

**Education:**

* Master of Science in Computers
* Bachelor in Business Administration, Major in Computer Information Systems
* Master’s in Business Administration, Major in IT Management

**Cyber Security Professional Affiliations:**

* **ISSA** Information Systems Security Association, USA

World Leading Cyber Security Professional Association

* **ISACA** Information Systems Audit and Control Association, USA

Leading Cyber Security Industrial Certifications Organization

* **SAN** Sys Admin, Audit, Network and Security, USA

The world’s largest cyber security research and training organization.

* **CISCO** Cisco Systems, USA

World Largest Cyber Security Infrastructure Manufacturer / Provider

**Professional Trainings and Courses:**

* Cyber Security Risk Management, Deutsche Bank NYC, USA
* Cyber Security Governance, Risk and Compliance, Deutsche Bank NYC, USA
* FISMA Compliance, Deutsche Bank NYC, USA
* CISO Compliance and Audit, Deutsche Bank NYC, USA
* CISO Principles and responsibilities, Deutsche Bank NYC, USA
* Firewall / IT Governance, Deutsche Bank NYC, USA
* Endpoint Security & Cisco ISE Management, TD Bank MI, USA
* NIST /PCI/DSS Standards and practices, TD Bank MI, USA
* Cyber Security Project Management, CPMI NJ, USA
* Data Centre Cyber Security Design, Alrajhi Bank, KSA

**Certifications:**

* **CISM** Certified Information Security Manager, ISACA USA
* **CRISC** Certified Risk & information systems Controls, ISACA USA
* **CISA** Certified Information Systems Auditor, ISACA USA
* **CCNPS** Cisco Certified Network Professional Security, Cisco Networks
* **CCNA** Cisco Certified Network Associate R/S, Cisco Networks
* **ACE** Associate configuration Engineer, Palo Alto Networks
* **MCSE** Microsoft Certified System Engineer, Microsoft Corp

**Professional Experience:**

**DELTA SYSTEMS, USA Jan 2024 – Till Date**

**Lead Cyber Security Architect / V CISO**

Lead Clients and their Requirements for Cyber security strategies, Planning, Designing, Testing, Implementing and Maintaining Cyber Security Infrastructure include Corporate Data Centers to protect the Complex / critical high level security Infrastructure includes Cloud Security, Applications Security, IOT (Internet of things) Etc.

**Responsibilities:**

* [**Designing Resilient Security Architecture**: Responsible for planning, studying, and designing robust security architectures for clients.](https://www.infosectrain.com/blog/roles-and-responsibilities-of-a-security-architect/)
* **Design and Implement Cyber Security policies, standards, procedures, and Cyber security controls.**
* **GRC**
* [**Implementing Security Controls**: Design and provide technical advice on the implementation of security controls, Cyber security Policies, frameworks implementation such as, **MITRE ATTACK, NIST, ISO 27001, PCI DSS**, **SABSA and TOGAF** across corporate and business systems.](https://www.velvetjobs.com/job-descriptions/principal-security-architect)
* **Risk Assessment and Vulnerability Analysis**: Supervise / Perform vulnerability assessments, security testing, and risk analysis to identify potential threats and vulnerabilities.
* **Cyber Security Intelligence: Research and deploy the best techniques and policies to protect Critical Cyber Systems to prevent Cyber Attacks.**
* **Leading Security Teams**: Lead teams of security Engineers, ensuring that security measures are effectively implemented.
* **V CISO / Information Security Management**
* Manage Risk Management controls include Third Party Risks
* Application Security Management
* Identity and access management
* **Cyber security Research and Training Development to Customers**
* Cloud Security design and operations
* Cyber Security Governance, Risk and Compliance
* Cyber Security Audit
* **Working Technology Vendors: CISCO, PALO ALTO, IBM, AWS, MICROSOFT, GOOGLE, NIST, ISO, PCI-DSS, METRE ATTACK, SPLUNK**

**CISCO, SANJOSE CALIFORNIA, USA February 2022 – November 2023**

**MANAGER I Cyber Security Engineering I Risk Management I Change Management I Cyber Security Project / Program Management**

**Responsibilities:**

* **Responsible for Intellectual Assets Protection Management (Cyber Security) 65 Security and IT Infrastructure and Builds**
* Supervise Global Security architects in build Existing security infrastructure, Remediation, and hardening process.
* **Lead Risk Assessment process and operations of 65 Security infrastructure and Build Environments**
* **GRC**
* Manage Teams of Cyber security / Build Security for Upgrading and design new security infrastructure
* Lead Application Security process and operations.
* Involved in New Cyber Security infrastructure design and deployment phases.
* Manage cyber–Security Risk Assessment, Compliance, Audit and Program Management
* **GRC Policies using MITRE ATTACK, NIST, ISO 27001, PCI DSS, SABSA and TOGAF**.
* Establish and maintain the Cyber Security program management guidelines.
* Routine Trainings to team lead include new security infrastructures and Security awareness Trainings.

**AL RAJHI BANK HO, KSA November 2019 – December 2021**

**Senior Manager**

**Cyber Security / Information Security**

**Responsibilities:**

* **Manage CISO: Chief Information Security Officer**
* **Cyber Security Design, Strategy, Planning and Governance**
* **Information Security Policy Management**
* **Risk Management and Incident Response**
* **Information Security Controls**
* **Information Security Audit**
* **Governance, Risk and Compliance**
* **IOT**
* **Leadership and People Management.**
* **Cyber Security Program Management**
* Assist with the overall business technology planning, providing current knowledge and future vision of technology and systems.
* Implements security controls, risk assessment framework, and program that aligns to regulatory requirements.
* Evaluates risks and develops security standards, procedures, and controls to manage risks. Improves PCC’s security positioning through process improvement, policy, automation, and the continuous evolution of capabilities.
* Review and Update **CISO Policies** twice a year.
* Implements processes, such as GRC (governance, risk, and compliance), to automate and continuously monitor information security controls, exceptions, risks, testing. Develops reporting metrics, dashboards, and evidence artifacts, **using frameworks MITRE ATTACK, ISO 27001, PCI DSS, SABSA and TOGAF**
* Information Security Awareness / Business continuity Management
* Updates security controls and provides support to all stakeholders on security controls covering internal assessments, regulations, protecting Performs and investigates internal and external information security risk and exceptions assessments. Assess incidents, vulnerability management, scans, patching status, secure baselines, penetration test result, phishing, and social engineering tests and attacks.
* Develop, implement, and monitor a strategic, comprehensive enterprise information security and IT risk management program.
* Work directly with the business units to facilitate risk assessment and risk management processes.
* Documents and reports control failures and gaps to stakeholders
* Provides remediation guidance and prepares management reports to track remediation activities.
* Facilitate IT auditors and Perform internal ISD audit.

**DEUTSCHE BANK, 60 WALL NEWYORK, USA June 2017 – November 2019**

**Senior Engineer**

**Cyber Security, Chief Security Office**

**Responsibilities:**

* **Lead Global Team of CSO Governance, Risk, Compliance and Security controls.**
* Involved in implementing and designing **CISO policies.**
* **GRC**
* Responsible for Firewall Governance, information Security Controls, IS Policies, Procedures, Risk, Compliance
* Investigated and effectively responded to security incidents and breaches.
* coordinating with incident response teams for containment and mitigation
* Firewall Connectivity Approvals, Audit and Security Awareness programs.
* Supervise Application owners for application security requirements and approvals.
* Design and Instructions Security awareness trainings to employees.
* Coordination with Network / infrastructure Consultants regarding security policies Implementation
* Monthly Analytics for CISO Global Operations.

**TD AUTO FINANCE MI, USA (Division of TD BANK) February 2017 – April 2017**

**Senior Security Engineer**

**Cyber Security / Network Security**

**Responsibilities:**

* **Lead Network Security Operations include**:

Palo Alto 5500 Firewalls, End point, ISE Vulnerability/ Scanning (Qualys) **Bluecoat** web proxySecurity infrastructure change management

* **Lead Cyber Security Operations include**:

Monitor network and application performance to identify irregular activity.

Perform regular audits to ensure security practices are compliant.

**RCSC RIYADH, KSA / UAE / OMAN / QATAR**  **May 2010 – December 2016**

**Senior Manager Cyber & Information Security**

**Responsibilities:**

* Administer and maintain Cyber Security policies to assure the safety and Security of Cyber Security Infrastructure
* Develop policies and procedures to protect enterprise communications, systems, and assets from internal and external threats.
* Create disaster and/or crisis preparedness plans.
* Responsible for overseeing an organization's overall cyber security.
* Supervises aspects of Cyber security including design, development
* **Cyber Security Governance, Risk and Compliance.**
* Cyber Security Project Management
* implementation, incident response and Threat Intelligence
* Budgets, and adherence to various regulations.
* Assist in building relationships with vendors and creating cost-efficient contracts.
* Analyze the business requirements of all departments to determine their technological needs.
* Coordinate IT managers and supervise computer scientists, technicians, and other professionals to provide guidance.
* Recruit, train, and schedule security personnel.

**ROYAL INSTITUTE OF COMPUTERS, CANADA March 2009 – April 2010**

Lead Instructor **Cyber Security & Systems Security**

**Responsibilities:**

* Responsible for instruction and course preparation
* Responsible for developing instructional materials, grading, and assessment.
* Professional responsibilities as a member of the instructional team
* Provide guidance and support to students in Computer labs include **Cisco and Microsoft**

Cyber Security and infrastructure solutions.

* Supervise Students in External Internships, Projects, and Specialized Thesis.

**CYBORG IT CONSULTING, CANADA January 2009 – April 2010**

**Principal Engineer Cyber Security / IT Security**

* Provide security guidance on a constant stream of new backend/core infrastructure and technologies.
* Analyze, assess, and respond to various internet threats.
* Interact directly with the security community regarding infrastructure security vulnerabilities and threats.
* Routine Operations of Firewalls and Proxy Servers
* Deliver ultra-high availability of Alcatel Telecommunications switching system security and access management.
* Participate in requirements/control definition, implementation design, build and staging,
* Verification and transition to maintenance and support.
* Design, configure, and support security deployments including Firewalls, Proxy servers and Windows server.

Routine meeting with Clients related to Network and system Security related issues.