Phone: +91–7680960759
E mail: shabeerk1@aol.com

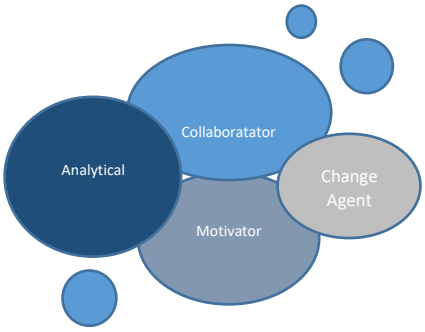
Shabeer Ahmed Khan, CISSP, CISM, ISO 27k, CEH, COBIT 5.

Target-oriented Cyber Security professional, pursuing Senior Managerial Assignment in Service Deliver, Information Security Risk Management Governance, Compliance (GRC) etc.

Profile Summary

- Sr. Cyber Security Consultant Specialist possessing 17+ years of rick work experience in Cyber Security Service and Delivery, GSOC (SIEM) Security Operation Management, Cyber Security Architecture and Design, Information security Risk management, Governance and Compliance (GRC).
- Hold certification like CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security anager), ISO 27001 Lead Implementer, CEH, SABSA (SCF Chartered Foundation), COBIT 5, ISSMP (Information System Security Management Professional) etc.
- End to end management of Cyber Security / IT Security Service Delivery which entails GSOC (SIEM), Firewalls, IDS/IPS, Web Proxy, IAM and PAM, Endpoint security, Vulnerability Assessment etc.
- Proven acumen in establishing Security Policy, procedure and security strategy,
- Third Party Risk Management (TPRM), and Security audits etc.
- Insightful knowledge of Information security framework like ISO27k, NIST, COBIT, SAMA (Saudi Arabian Monetary Authority) etc. Establishing security strategies and controls to mitigate organizational risks.

Soft Skill



- Displayed credentials in heading the US, Europe, Nigeria, India and Oman. Leading a team of 14+ Individual leads Managers and advisory while working as (Cyber Security Consultant, ASO for DXC, SOC Consultant Manager for Zentic Technologies).
- Revised and significantly improved the information security practice; perform security risk assessments in line with global best practices and implemented remediation measures adopting appropriate controls enhancing effectiveness & quality of service delivery.
- Excelled at delivering various onsite assignment in Nigeria and Oman conducted Risk Assessments, IT infrastructure audits and Security projects sign off etc. in the role of ASO and SOC Consulting Manger.
- Conducting various Information Security awareness sessions recommending mitigation through appropriate controls.
- Worked as an advisory to CISO and Board Members to Bank with DXC technologies.
- Directed broad range of service delivery initiatives through planning, analysis, and implementation of security solution which yielded excellent outcome as a business to DXC.

Core Competencies

Service Delivery Management
Cyber Security Operations
IT Security Management GSOC (SIEM)
IT Governance, Risk & Compliance
Project Execution & Implementation
Threat/Vulnerability Management
Incident & Problem Management
ISMS /Risk Assessment /ISO27001
Leadership& Team Management
IT Architecture and Design
SIEM Tool's
Agile & Waterfall Methodologies

Career Timeline

- IT Manager Kaza Medical Group (Dover U.S) April'03–Feb'07
- Sr. Network Engineer VoiceGate India Technologies Mar'07–July'08.
- SOC Manager Zentic Technologies Aug'08-Oct'10.
- Sr. Network Security Manager Incessant Technologies Nov'10-May'11.
- Sr. Security Consultant RBS Wipro Technologies Jan'12-Aug'14.

Organisation Experience

Dhofar Power Company (DPC) Oman, Feb'19 – till date
Sr. Cyber Security Consultant, Oman

Key Result Areas:

- Sr. Cyber Security Consultant for the entire DPC (Dhofar Power Company) Cyber Security, Information Security & Risk Services wherein the technology landscape spares across SOC, Patch Management, Vulnerability Management, Firewall IPS/ IDS, NAC, Endpoint Security/ Antivirus, DLP, Web proxy etc.
- Implementation of Policy and procedures as per ISO 27001\27002 to Governing ITSM.
- Responsible for Delivering Security Management of entire DPC Oman within the region within the Managed security NIST \ ISO 27k delivery model, manage a team of 9+ which contains of multiple Project managers, architect and Team leads and advisory to SCADA Team including Board of Directors.
- Established Cyber Security TAC and made many non-functional to in line with stake holder's expectations.
- Directly managed multiple ongoing projects and operations.
- Leading and contributing to the security posture of DPC networks and systems, data centre infrastructures, IT architectures and solutions.
- Serving as a Cybersecurity expert to contribute to the definition/development of overall IT architecture.
- Take responsibility for working with assigned technology streams and business led projects assigned to you to ensure they are aligned with DPC Security Policies, Architecture design principles, Technical Security Requirements and other required internal/external standards.
- Developing, contributing and management of Security Architecture Specifications, Security Architecture Analysis, Threat-Modelling, Security Requirements, Security Standards and Design Patterns, Reference Architectures, Security Strategies and Roadmaps
- Applying security framework principles to developed & support security solutions.
- Providing strategic points of view for security solutions and security industry events.
- Played step bar role in effective handling customer escalations and maintaining customer confidence in delivery.
- Managing the lifecycle of security technologies.
- Working closely with the other technology architects to ensure that security is properly embedded in their technology domains architectures.
- Advising leadership on Cybersecurity issues, systems, processes, products, and services.
- Maintaining oversight of the design and implementation of IT systems & services to ensure appropriate and effective security controls are included.
- Serving as a Cybersecurity expert to contribute to the definition of overall IT architecture.
- Reviewing current system security measures and recommending and implementing enhancements
- Conducting regular system tests and ensuring continuous monitoring of network security
- Developing project timelines for ongoing system upgrades
- Fortnight account review with the respective Board of Directors and IT Head, to ensure delivery hygiene, maintaining Risk trackers / escalation trackers and enable them to resolve Cyber Security and IT Risk issues.
- Monthly Cyber security review with key customer stake holders of various branches across Oman.
- Displayed excellent leadership credentials in Cyber security strategy, handling disputes and monitoring and uplifting of team.

DXC Technologies – Mumbai (SIDBI and Banka of Bank Of Baroda) Jan'17 -Feb'19
ASO (Account Security Officer) – Projects & Service Delivery (Cyber Security & Enterprise Risk & Governance)

Key Result Areas:

- End to end management of Cyber Security / IT security service delivery that include SIEM tool (IBM Qradar, Splunk, Micro focus ArcSight, Firewall, IPS/IDS, Endpoint Security Antivirus Identity and access management, application security testing and static code analysis, (fortify), vulnerability assessment (Nessus, Nmap) with Kali linux IBM AppScan and Proxy.
- Leading a team of 16 people including Security Analyst, SME Engineers and Team leads and supervising around 46 people within the vertical.
- Driving Security Advisories to CISO and Board Members. Threat Intelligence and GSOC Automation Initiatives within IT Security vertical.
- Analysis of IAM configuration and policies to identify security and operational gaps.
- Review and govern the services-based Integration (i.e. REST, APIs), role-based access control, Active Directory, LDAP, Single Sign-On, End-User provisioning, IAM governance, and identity data synchronization services with existing enterprise applications and systems.

- Advisory for security related assessments and configurations for Identity and Access platforms, adaptive risk configurations and Multi-factor authentications
- Define and setup approach for risk-based MFA and application access control.
- Assist with remediation of mis-configuration identified by information security team on IAM & PAM platforms.
- Govern and improve IAM processes and posture of the organization alongside the platform deployment with configuration reviews and recommendations meeting business requirements.
- Develop and report identity governance, SoD and risk metrics as well as reports and scorecards consumed by management.
- Keep pace with emerging IAM and PAM technology, cyber threats, and industry trends around cybersecurity.
- Develop enterprise wide standards for IAM, Privileged Account management to meet business requirements.
- Employee should stablishes and refines procedures and other business processes to detect errors and inconsistencies in privileges.
- Support detailed reporting and root cause analysis with various internal technology teams. Build relations and serve as a liaison between system/application owners and the IAM internal technology team for governance and security specific initiatives.
- Creating & executing service improvements across multiple projects to mature overall service delivery
- Administering overall security compliance aspects of the project, ensuring adherence of practice to global security framework like ISO 27K, SANS, NIST, COBIT and so on by executing internal audit within vertical.
- Presenting multiple senior management presentations with Senior Directors, Vice Presidents and Key Stakeholders form client end.
- Creating and sustaining a dynamic environment that fosters development opportunities and motivates high performance amongst team members.

Highlights:

- Received excellent feedback from the “customers” and extension of the contracts.
- Achieved excellent result through development & execution of employee retention strategy.
- Implemented and coordinated the strategy to optimize SIEM and end point service delivery
- Proposed and implemented multiple service improvement with the IT Security services which received very good appreciations from key stake holders.
- Conducted various internal audit including (SWIFT) and ensured adherence of the project to global best practices.
-

Ace Clouds, Hyderabad. (Nigerian bank First Bank of Nigeria, & United Bank of Africa) onsite Nigeria Sr.IT Security Manager Sep'14–July'16.

Key Result Areas:

- Creating and managing security strategies.
- Framing robust IT security policy and implementation.
- Provide IT security awareness training to organization personnel.
- Oversee information security audits, whether performed by organization or third-party.
- Manage security team members and all other information security personnel.
- Assess current technology architecture for vulnerabilities, weaknesses and for possible upgrades or improvement.
- Implement and oversee technological upgrades, improvements and major changes to the information security environment.
- Manage and configure physical security, disaster recovery and data backup systems.
- Monitor all operations and infrastructure.
- Maintain all security tools and technology.
- Monitor internal and external policy compliance.
- Work with different departments in the organization to reduce risk.
- Audit policies and controls continuously.
- Ensure cybersecurity stays on the organizational radar.
- Detail out the security incident response program.
- Conducted various third party risk assessment (TPRA), cloud security assessments, Application Security assessment etc.
- Performed security assessments prior to on boarding new operational entities to FBN & UBA.
- Attended NBMs (New Business Meetings) and recommended stakeholders on security relevance of project& ensured sufficient budget had been allocated for fulfilling security requirements.
- Conducted various gap analysis, risk assessments and audits to establish ISMS within the organization and obtain ISO27001 certification.
- Drafted risk profile & risk treatment plan for FBN & UBA IT Ops division and completed internal audit to ensure compliance.
- Completed ISMS Roll-out Project adhering to strict timelines by working in lock step with leads & managers.
- Imparted trainings & awareness sessions to team leads on ISMS Implementations Methodology, security
- Policies/ standards and information security best practices.
-

Wipro Technologies, Bangalore (RBS Royal Bank of Scotland)
Sr. Security Consultant Jan'12-Aug'14.

Key Result Areas:

- Supervised all security services outsourced from India including SOC (SIEM) & application security assessments in line with OWASP guidelines.
- Highest ability to execute, from strategy and implementation to operations.
- Ensure that the organization's strategic plan, mission, vision, and values are communicated to the relevant parties and integrated into the strategies, goals, objectives, work plans and work products and services.
- Serve as a principal contact for coordination, implementation, and/or enforcement of Cyber Security.
- Implement higher-level security requirements and integrate security programs across disciplines.
- Initiate, develop, implement, and evaluate the security programs of an organization.
- Make recommendations for operational policies, procedures, and criteria for interfacing with program systems resources, and coordinate with other members of Wipro as well as our customers on the development of information security systems and application policies.
- Ensuring all personnel have access to the IT system limited by need and role
- Establishing disaster recovery procedures and conducting breach of security drills
- Promptly responding to all security incidents and providing thorough post-event analyses
- Daily interface with UK Stakeholders IT organizational and internal IT organizational leadership.
- Liaised, led & implemented SOC related activities like security monitoring, security incident management, triaging & escalations and delivered administrative & technical support for SOC operator personnel 24/7
- Ensured efficiency in operations and met of individual & group target by leading mentoring & monitoring the performance of SOC team members.
- Managed the 24/7 vulnerability assessment operations in collaboration with manual testing ensuring quality results.
- Managed Penetration testing request from various customers by ensuring utilization of the available resources effectively.
- Conferred with 'RBS Service Excellence Award' for outstanding performance & dedication.

Sankhya InfoTech Pvt Ltd, Hyderabad. July'11 – Dec'11.
Sr. NOC Manager

Key Result Areas:

- Responsible for driving various daily, weekly calls like Service Review, Backlog, Compliance, Transition etc.
- Manage and Mentor a diverse staff of 24x7 technical resources which includes off-shore.
- Responsible for customer marketing to increase revenue for the internal business and the customer while being cost conscious. Consistently exceed customer and internal growth projections.
- Perform security risk assessments on existing company assets and new emerging technologies Provide guidance for the development and implementation of security policies for all Sankhya customers.

Incessant Technologies **Hyderabad** Nov'10 - May'11.
Sr. NOC Manager.

Key Result Areas:

- Handle formal escalations (technical & non-technical cases) handed over by Global Escalation Management Team.
- Handle internal escalations (technical & non-technical cases) escalated by Tier-2 & Tier -3 Technical Support Engineers both locally and from global teams.
- Liaise with RSA Professional Services (Consulting) and Virtual Service Delivery (Implementation) teams and participate in implementations and escalations (both internal & external) when on-demand solutions are needed.
- Conduct webinar sessions on a quarterly basis for client on product features, functionality, configurations and basic troubleshooting skills so as to increase understanding of the product and the underlying technology.
- Conduct Brown-Bag sessions on a monthly basis to train the team members on various technologies to increase their technical acumen and overall skill sets.
- Participate in the Manager's Ops Review meetings and conduct team meetings on a weekly basis there by ensuring a smooth flow of information from management to the team members with regard to process and strategies on case handling, customer handling and CSAT.

Zentic Technologies **Hyderabad** Aug'08 – Oct'10.
SOC Manager

Key Result Areas:

- Responsible for Threat Detection and Response actions efficient in handling of SOC operations to improve the security posture of the organization.
- Strategize with leadership on the direction of the security operations program.
- Build an efficient Security Operation Center (SOC) and manage security operations staffs
- Serve as the escalation point for technical analysis and response by leveraging superior technical knowledge of adversary tactics, techniques, and procedures.

- Stay up to date with news and trends in information security including new vulnerabilities, methodologies, and products.
- Command incident response efforts and be able to correlate multiple data sources applying various analytical techniques.
- Create and track investigations to resolution as needed both internal to security operations as well as holding other department members accountable.
- Holistically deploy, maintain, and tune new security controls and alerts critical to the security mission of the organization.
- Work with other teams to identify, resolve, and mitigate vulnerabilities and risks.
- Work with vendors and other third parties independently in pursuit of program goals.
- Generally, works to solve security challenges at scale while balancing usability, stability, scalability and performance.
- Define and track SOC metrics KPIs
- Detailed understanding of advanced tactics and methods used in Cybercrimes, Hacktivism, and APTs
- Ability to interpret highly technical data and perform detailed data analysis slicing & dicing
- Two clients staged for initial ISO 27001 certification audits.
- ISO 27001 ISMS Readiness Evaluations (non-implementation clients)
- Conducted independent evaluations of organizations ISMS to determine readiness for certification.
- Document and assess enterprise application systems and interfaces, and identify key controls.
- Develop test plans, test controls, identify remediation issues, and recommend principals and best practices.

VoiceGate India Technologies. Hyderabad March'07 - July 08.

Sr. Network Engineer

Key Result Areas:

- Handle technical issues related to remote connectivity (dial-up, ethernet and Wi-Fi) with the iPass Connect client for enterprise customers from all over the globe.
- Assign cases logged by enterprise customers from the ticketing system (REMEDY) and work with the customers' engineering & network teams to resolve complex issues pertaining to new client builds and configurations, existing client modifications and providing resolutions to any and all possible remote connectivity issues as a Tier – 2 engineer.
- Replaced legacy equipment with state-of-art hardware
- Accurately identified and labeled assets to simplify future troubleshooting
- Optimized operation due to better airflow and ventilation in server areas
- Investigate and resolve billing issues logged by the customers' due incorrect pricing plans, provider issues and also investigate fraudulent usage as and when reported by the customers'.
- On a regular basis co-ordinate with the Tier – 3 engineers, Account Managers, Network Services Team and the Billing Department and ensure the smooth flow of process across all teams across all time zones.

Kaza Medical Group (Dover lakeside U.S) April'03 – Feb'07

IT Manager (HIPPA Security)

Key Result Areas:

- Leading a Team Head of 48 people. Motivate them & influence them positively ensuring that the team performs according to the set standards and established goals.
- Handle HIPPA compliance and mitigate those compliance issues.
- Manage and deliver IT transformation projects from the early planning phase through the successful deployment.
- Assess the current state of clients' infrastructure, develop security strategies and roadmap for improvement and advise in further securing the clients' IT environments and interaction with their on-premise infrastructure.
- Assist clients in developing strategies to secure their environment by providing high value consultancy work.
- Train the team members on new technical updates & conduct proof of learning periodically.
- Participate in Joint Calibration Sessions with the Quality Team following HIPAA Compliance (4010- 837/835, 276/277).
- Awareness Security Training to US counterpart for Doctor's and other team mate's.

Certifications:

B.Com Computers 2003

Certified:

CISSP – Certificate No: 348340
CISM – Certificate No: 258745 (Expired)
SABSA (SCP) – Certification No: SCP11101489 (Expired)
ITILV3 (ITSM) Foundation
ISO27001:2013 Lead Implementer (EC-Council).
CEH 9 –Certified Ethical Hacker
COBIT 5
CCNA -2003 (CISCO)
MCSA – 2003 (Microsoft Certified System Administrator)

Personal Details

Date Of Birth: 21st Feb 1979
Languages Known: English, Hindi.
Permanent Address: Malkajgiri Hyderabad, India.

S Ahmed Khan