IHSAM KHAN

Mobile: +97334143455, Pak: +923005646596
Email: ihsam_khan89@live.com
Skype: ihsam.khan
BSSE- Software Engineering

CAREER OBJECTIVES:

Seeking an opportunity where my skill set, and energy can be put to maximum use for the mutual growth of the organization and myself. My objective in my profession is to put my best whatever I do. The understanding coupled with my creative analytical abilities and hard work has always been my strong suite. Having a professional degree of Bachelor in Software Engineering along with strong credentials including Certified Information Security Manager (CISM), ISO 22301- Lead Implementer BCMS, EC-Council Certified Ethical Hacker (CEH v10), EC-Council Certified Incident Handler (ECIH v2) and with various industry leading certifications training like CISSP. I have professional expertise in implementation and management of ISO 27001-2013, Risk Assessment and Management, GAP assessment, GDPR and Bahrain Personal Data Protection Law (PDPL), NESA standards, PCI DSS ,SWIFT CSP internal auditing(Gap Assessment), Incident Response and Handling, Disaster Recovery Planning, crisis communication and governance, risk and compliance (GRC).

SKILLS:

ISO 22301:2019 BCMS-Implementation
ISMS -ISO 27001-2013 (Implementation and Auditing)
Logs Management
Application Firewall
VAPT (manual and automated)
Security Incident and Response
SWIFT CSP
Security Assessment & Patch Management
Solar Wind PaperTrail
Personal Data Privacy Law
NIST C-SCRM
Disaster Recover Planning
Gap Assessment and IS Advisory
Business Impact Assessment
Incident Management
Business Contingency Planning
Risk Management-ISO 27005
IS Governance, Risk and Compliance-GRC
SolarWinds LEM
GDPR
NIST SP-800-53
Linear Tracking Tool

PROFESSIONAL EXPERIENCE:

Baker Tilly Middle East **Nov 2019- To Date**
Information Security Consultant

- Strong knowledge of information security frameworks and standards with hands-on implementation and internal audit.
- Designed a complete set of Policies and Procedures against ISO 27001/2.
- Designed Statement of Applicability document against Controls ISO 27001/2 – Information Security Management System Standard.
- Performing detail gap assessment for client evaluation.
- Conducting Business Impact Analysis (BIA) identifying critical systems, facilities to internal organizations and processes.
- Designed a detailed risk management framework based upon ISO 27005 – Risk Assessment Standard, NIST SP 800-30, Factor Analysis of Information Risk (FAIR) and Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE).
- Carried out Asset Identification, Asset Classification, Vulnerability assessment, Threat Identification, Business Impact Analysis, Risk Assessment, followed by Risk Treatment Plan.
- Designed a Statement of Applicability document and complete set of Policies and Procedures against ISO 22301-2012/2019.
- Determined the critical business functions by conducting interview sessions with the business process owners
- Determined suitable RTO, RPO, WRT and MTD after discussion with BPOs and Management
- Designed a detailed disaster recovery strategy based upon the business requirement and cost.
- Designed a detailed Crisis Management and Communication Plan, strategy and activities like crises matrix, crisis management, crisis communication, command, and control center.
- Revise and update ISMS, IT policies and procedures to comply with the requirements of NESA.
- Maintain and implement NESA compliance requirements for information assets and supporting systems.
- Review client IT and IS policies, procedures, and access controls to ensure compliance with NESA best practices.
- Conducted Information Security Awareness Sessions enterprise – wide.
- Designed a complete Information Security Awareness Framework.

- Designing attractive tips on pre-decided issues of information security and releasing periodically via Email and centralized portal organization wide.
- Conduct regular audits in compliance with all ISMS policies and procedures on behalf of the IS Governance Team.
- Identify Incidents for review and keep users informed about their Incidents' status at agreed intervals
- Information security support to Bahrain Development Bank for Office 365 and AWS Cloud migration.
- Review client IT policies, procedures, and access controls to ensure compliance with best practices.
- Information security and ORM Cyber Security gap assessment as per compliance requirements.
- Analyzed security controls, gap assessment and data privacy impact assessment (DPIA) for Bahrain Development Bank-Data Protection Law (DPL).
- Personal Data Protection Law and information security gap assessment for banking clients and address non-compliance strategies.
- Information security best practices support for core banking application and World Check One (AML alternative).
- Develop and implement information security contract clauses for Bahrain Development Bank.
- Working on Solar Wind log analysis and management tool for core IT infrastructure for Khaleeji Commercial Bank.
- Information security assessment and support for KHC-Aggregator (Khaleeji Commercial Bank-Mobile Banking Application) for eazyNet™ Biometric Services for Khaleeji Commercial Bank.
- Conduct backup review, access control assessment and system authorization verification and review exercise for banking clients.
- Hands on VAPT and perform infrastructure and application penetration tests, as well as physical security review and social engineering tests for clients.
- Perform application penetration tests across public and private network.
- Develop processes, activities to implement tools and techniques for ongoing security assessments of the environment.
- Analyze vulnerability test results, reporting and develop targeted testing as deemed necessary.
- Actively involved in application secure development lifecycle activities, process assessments and evaluate security pasture from time to time.
- SWIFT customer security program (CSP) gap assessment/SWIFT internal audit.
- CSAT gap assessment for Office 365 migration.
- Identify and prioritize security and fraud controls to be implemented.
- Developing and designing cybersecurity assessment and periodic inspection reports for CBB compliance requirements.
- Proficient in understanding and assessing application level vulnerabilities like XSS, SQL Injection, CSRF, authentication bypass, weak cryptography, authentication flaws etc.
- Hands on experience using variety of security tools like Kali - Linux, Wireshark, , Nessus and Open Vas.
- Experience in different web application security testing tools like Metasploit, Burp Suite, Sqlmap, OWASP ZAP Proxy, Nessus and Nmap.
- Sound experience in Vulnerability Assessment and Penetration Testing on WEB based Applications and Infrastructure penetration testing.
- Hand on experience in Secure SDLC and Source Code Analysis (Manual & Tools) on WEB based Applications.

Ministry of Interior, Bahrain **Sept 2016– Nov 2019**
Information Security Officer

- Administrating and securing IT servers and infrastructure.
- Responsible for backup, storage and data security as per required standards set by MOI Bahrain.
- Performing the operational establishment and preventive maintenance of backups, recovery procedures, and enforcing security and integrity controls.
- Engagement with technical process owners from respective organizations to identify risks and drive towards a completed documentation that aligns with the IT Governance and Risk Management programs
- Conducting Risk assessment, developing and maintaining risk register and designs self-assessments to help identify risks and to support security infrastructure.
- Performing VAPT exercise and research activities to investigate vulnerabilities and technologies which may impact security posture.
- Performing Information Security policies, procedures review and gap assessment. Also responsible for the processes, procedures and operational management associated with system security and recovery.
- Installing, configuring, updating and maintaining the security software and applications such as antivirus software.
- Troubleshooting and providing service support in diagnosing, resolving and repairing server-related hardware and software malfunctions, encompassing workstations and internal communication infrastructure.
- Support, monitor, test, and troubleshoot hardware and software problems, implementing and administering system security and managing security tools.
- Periodically performing access control review exercise for critical and non-critical IT infrastructure.
- Implementation and ensuring appropriate security controls for data and system access.
- Providing support to the users and solving the queries in data handling.
- Liaising with vendors, suppliers, service providers and external resources analyzing, recommending, installing and maintaining system and applications security; and monitoring contractual obligations, performance delivery and service level agreements.
- Act as administrator for a variety of systems-related security and monitoring network activity to identify issues early and communicate them to network team.

- Subject matter expert on all information security and processes including monitoring the systems continuously for malware, viruses and other intrusions as per required standards set by MOI, Bahrain.
- Document all activities during any incident and provide support with status updates during the incident life cycle.
- Engaged with software development teams during SDLC for secure by design development so that the data in the applications can be accessed safely, like Stamp System of MOI,Bahrain
- Also work as member of Information Security Awareness Team in the organization.

Telconet Services Pvt Ltd, (Pakistan) **Oct 2015 - May 2016**
Database Administrator/ MIS Developer
- Centralization Software System (CSS) Pakistan Post

Khan & Co, Distributor Pakistan Tobacco Company **June 2013-June 2014**
Associate Database Administrator
- Supply Chain Order and Stock Maintenance (SCOSM)

CERTIFICAITONS / TRAINING/EDUCATION:

- Bachelor's in Software Engineering (BSSE), International Islamic University, Pakistan
- Certified Information Security Manager (2158212)
- ISO 22301 Lead Implementer- Business Continuity Management (BCLI1068159-2021-01)
- Certified Ethical Hacker (CEH v10) EC- Council (ECC4321078596)
- Certified Incident Handler (ECIH v2) EC-Council (ECC1967235408)
- Certified Information System Security Professional (CISSP-Candidate)
- Cisco Cyber Security Essentials(certified)
- Cisco Cyber Security Fundamental (certified)
- R12.x Install/Patch/Maintain Oracle E-Business Suite
- Oracle Database 11g Administrator Certified Professional

REFERENCES:

- Muhammad Ali Salahuddin Dar, Senior System Security Administrator, **ma.dar@interior.gov.bh** ,(+97366331113)
- Muhammad Wasim Mahmood, Network Administrator, **wk.mahmood@interior.gov.bh** ,(+97339082008)
- Muhammad Nawaz, Senior ICT Projects Manager, **mnavaz@interior.gov.bh** ,(+97339954044)
- Muhammad Umair Ahmed, Manager-Information Security, **uahmad@bakertillyjfc.com**, (+97334045544)