ZAHRA ALWARSH

Dammam, KSA ● (966) 541413135 ● Zsag2d@gmail.com

CAREER OBJECTIVE

An **accomplished Cyber Security professional with over 5+ years of progressive experience** building teams and managing secure IT operations within complex insurance corporate cyber security working environments. Proven expertise in **implementing cyber security measures, troubleshooting network infrastructures and allocating staff resources/trainings**. Impeccable record of delivering security improvements, evaluating and identifying vulnerabilities and improving overall system efficiencies. Impressive capacity to thrive in fast-paced environments while delivering quality results.

- **Registered success in developing and implementing SAMA Cyber Security Framework** along with appropriate cyber security governance, robust infrastructure and all necessary detective and preventive controls to withstand cyber security threats.
- **Proven analytic and problem-solving skills** with the keen ability to assess needs, define requirements, develop value-added implementations and execute technical solutions that streamline and improve operating efficiencies.
- **Demonstrated great depth in business-driven technology design, delivering agile, flexible, and scalable solutions**, whilst striving to match the high expectations of flawless customer experience, continuous availability of services and effective protection of sensitive data.
- **Skilled in aligning end-user needs with long term resolutions while improving resilience against cyber threats.**
- **Quick learner, innovative individual who multi-tasks and has an excellent sense of teamwork** to get results by instilling commitment, trust, fairness, and loyalty. Strengths include solid communication and problem-solving skills and adapting to change combined with a passion to explore new technologies.

SKILLS

• Governance, Risk and Compliance	• Technical Innovations	• Business Alignment
• Encryption and Decryption	• Business Analysis	• Coordinating Departments
• Digital Signatures	• IT Infrastructure Management	• Leadership, Team building
• Public/Private Key Encryption	• Budgeting, Costing	• Motivation, Communication
• Vulnerability Assessment (Nessus)	• Standardizing Policies/Procedures	• Time Management, Ability to work under pressure
• ISO27001 Framework Monitoring Implementation	• System Analysis	
• Risk management	• Technology Integration/ Architecture	
	• Governance and Security	

PROFESSIONAL EXPERIENCE

Gulf Union Alahlia Cooperative Insurance   **Apr 2018 – Present**
Cybersecurity Manager (Acting)

Designation Chronology:
- Jun 2021- Present: Cybersecurity Manager (Acting)
- Apr 2018- Jun 2021: Cybersecurity Officer

Joined the organization as **Cybersecurity Officer** and moved up the corporate ladder to merit promotion to the position of **Cybersecurity Manager**.

Accomplishments- Cybersecurity Manager (Acting):
- Handpicked to develop and implement SAMA Cyber Security Framework in the organization within the required parameters and ensure compliance with the established framework.
- Demonstrated expertise in driving vulnerability management governance, leadership in vulnerability scanning solutions, e.g., Knowbe4, Nessus, Kaspersky EDR, etc.

Key Responsibilities - Cybersecurity Manager (Acting):
- Providing effective, high-quality services that support safe and secure networks, enforcing strict controls and checks on channels through which information flows into and out of an organization's information network.
- Defining technology solutions and roadmap; introduced modern business systems solutions by anticipating consequences of actions, potential problems which underline the need to safeguard sensitive data and transactions, and thereby ensure confidence in the overall Saudi Financial Sector.
- Planning and deploying tactical plans to supervise and track all operational workflow across the network and managing the infrastructure that facilitates those operations.
- Installing a robust cyber resiliency strategy, sourcing the best cybersecurity tools and advanced technologies for enabling the organization to effectively identify and address risks related to cyber security.
- Promoting cyber awareness with clients and project teams to build client trust and address key security and privacy concerns.
- Devising, implementing, and continuously monitoring critical vulnerability response processes to efficiently remediate critical vulnerabilities/incidents as well as installed strong security controls to ensure the protection of systems.
- Spearheading a team of 2-3 members and owning accountability of Applications Security for IBM Qrader, Nessus, Knowbe4, McAfee DLP, Kaspersky EDR, Darktrace and clearsky.

- Establishing comprehensive cyber hygiene and related best practices to keep sensitive data organized, safe, secure from theft and external attacks.

Accomplishments - Cybersecurity Officer

- Played a key role in implementing and monitoring the SAMA Cyber Security Framework, ensuring adequacy and effectiveness of internal controls as well as accuracy and completeness of reporting.
- Drove strategic programs, requirements & gap analysis, innovation, cyber resiliency, response, and technical implementation activities.
- Strove to achieve an appropriate maturity level of cyber security controls and ensure cyber security risks are properly managed within the organization and in alignment with the SAMA Cyber Security Framework.

Key Responsibilities- Cybersecurity Officer:

- Ascertained compliance with SAMA Cyber Security Framework, vital in identifying deficiencies and recommending actions to ascertain that AACI is compliant with the framework requirements.
- Provided inputs to update the internal Policies, procedures and standards and align all policies to the requirements of the regulatory Information Security, monitoring the same through periodic compliance reviews and prompt reporting.
- Responsible for the overall end-to-end management of the company's cybersecurity operations right from devising a robust Cyber Security Strategy, Plan, Policy through cybersecurity architecture as well as the governance, risk, and compliance.
- Performed gap analysis and developed continuous improvement of the core functions expected from the Cybersecurity Operations Framework, including threat detection and prevention, incident response, etc.
- Oversaw risk remediation activities, introduced risk-based solutions that address people, processes and technology. Presented reports on the progress of IS risk remediation activities, resulting from oversight and monitoring processes.
- Acted as a catalyst for change to improve security processes that benefit the organization, identified all cyber security requirements for each project/process; devised KPIs and KRIs for Cyber security maturity.
- Imparted training for employees to familiarize them with Cybersecurity knowledge as well as created innovative banners and emails to develop cyber security awareness among employees and clients.
- Maintained an effective compliance program through a structured Cyber Security Audit Plan in addition to carrying out risk assessments for cloud system and Monitoring SIEM solution by using Clearsky tool.
- Managed the risks against regulatory compliance obligations, as well as control framework commitments to their SAMA team. Presented SAMA with cybersecurity performance reports and updates on maturity level and controls implemented.

Almana General Hospital   **Nov 2017 – Mar 2018**
System Analyst

Accomplishments:

- Addressed the growing need for technology and accordingly updated Software Specifications.
- Provided the required impetus to improve business processes and offered first-level support to maintain top-notch applications functionality.

Key Responsibilities:

- Provided strategic leadership in transforming systems, modifying processes to meet new user requirements.
- Understood the current status of the systems, analyzed new business functional activities to compare them against standards, best practices and industry benchmarks. Suggested technical procedures and documentation for new/existing applications.
- Defined and implemented workflow automation and process improvement plans for the in-house developed systems and supported the development of system design and functional specifications
- Established technology roadmap, overall objectives and led application development projects.
- Contributed to planning, development and organization of systems/procedures and policies. Managed internal and external stakeholder expectations and ensured IT develops in line with corporate guidelines

Other Professional Experiences:

- Dec 2015 – Aug 2016: Manager Assistant, Almadloh Dispensary
- Jun 2010 – April 2011: Student Assistant, Missouri S & T International Office

EDUCATION

B.S. Business Management System, Missouri University of Science & Technology
Minor Information System & Technology – May 2015

Professional Development:
Professional Certification:

- Nov 2021: CISM (Certified Information Security Information), ISACA
- May 2021: IoT, Ministry of Communications and Information Technology

- May 2020: Intro to Cybersecurity, Atta Digital
- May 2020: Insurance Foundations Professional Exam, Financial Academy
- May 2017: Fundamentals of Cryptography, Cybrary
- May 2015: SAP (System, Application and Products) Certificate of Excellence, Missouri University of Science & Technology

Training Courses:

- 2020: Security+-, Udemy
- Nov 2020: IFCE Financial Academy
- Nov 2018: Certified Information Security Manager (CISM) training– Global Knowledge

PERSONAL INFORMATION

- Date of Birth:
- Marital Status:
- Nationality: