

VULNERABILITY MANAGEMENT | SECURITY ARCHITECTURE | APPLICATION SECURITY | NETWORK SECURITY

As a seasoned Senior Cyber Security GRC Specialist, highly proficient in conducting comprehensive risk assessments, identifying critical vulnerabilities, and implementing robust controls to safeguard organizational assets, including Operational Technology (OT) environments. With a proven track record of facilitating regulatory compliance and designing secure systems architectures, I am poised to excel in a Senior Cyber Security GRC Specialist role. Demonstrable in orchestrating successful security reviews for new applications, features, and OT systems, coupled with the ability to navigate complex GRC frameworks. Additionally, active membership in change advisory boards underscores my commitment to a proactive and collaborative approach to security governance, solidifying my position as a strong candidate for the Senior Cyber Security GRC Specialist role.

AREAS OF EXPERTISE		
Identity & Access Management	Security Metrics & Reporting	Programming & Scripting
Windows AD & Linux OS	Regulatory Compliance	Security Frameworks
Application Security	Penetration Testing	Business Continuity
Incident Response	Disaster Recovery	Incident Handling
3 rd Party Vendors	Risk Assessment	Cloud Security
Data Protection	Security Audits	OT Security

- KEY COMPETENCIES
- Problem-Solving:** Methodically uses logic and analysis to come to a solution
 - Communication:** Strong communication and data presentation skills
 - Critical Thinking:** Actively and skilfully analyses information collected from multiple disciplined processes
 - Adaptability:** Swiftly adjusts to changing settings and obstacles to suit the needs of the task at hand
 - Leadership:** Cross-collaboration, inclusiveness and diversity are valued
 - Relationship Building:** Works to build and maintain relationships in order to help achieve work-related goals

- SELECTED ACCOMPLISHMENTS
- Demonstrated expertise in developing comprehensive information security policies, creating a resilient framework for safeguarding critical assets
 - Spearheaded vulnerability management efforts, ensuring proactive identification and mitigation of security vulnerabilities to fortify organisational defences
 - Elevated the change management process by implementing strategic enhancements, streamlining procedures and minimising risk during system updates and modifications
 - Established efficient practices for processing application changes, enhancing operational agility while maintaining security standards
 - Introduced diversified security configurations, bolstering resilience against evolving threats and expanding the organisation's defensive capabilities
 - Attained industry certifications and cultivated deep expertise, contributing to a higher level of competency in information security and keeping abreast of the latest trends and best practices

CAREER SUMMARY

Senior Cybersecurity GRC Consultant

Saudi Electricity Company

KSA

December 2023 - Present

- Duties and Responsibilities:
- Conducts risk assessments for critical applications, identifying significant risks, thoroughly analyzing potential impacts, and strategically recommending appropriate controls to safeguard systems and data against potential threats.
 - Implements and enforces security controls within the OT environment, conducting regular risk assessments and monitoring to ensure that critical infrastructure systems remain resilient against cyber threats and comply with industry security standards.
 - Performs comprehensive cybersecurity reviews and approvals for new Proof of Concept (PoC) projects, systems designs, and architectures, ensuring adherence to security requirements before deployment.
 - Leads third-party risk assessments for vendors, meticulously evaluating and monitoring the security posture of external partners to ensure compliance with organizational security standards.
 - Develops and maintains Key Risk Indicators (KRIs) to monitor and measure risks, using these metrics to proactively identify potential security threats and implement mitigation strategies.
 - Creates periodic reports through Power BI, providing insightful data visualizations and analytics to senior management to support strategic decision-making.

Duties and Responsibilities:

- Meticulously conducts risk assessments for more than 65 critical applications. Identifies significant risks, thoroughly analyses potential impacts and strategically recommends appropriate controls to fortify our systems and data against potential threats
- Conducts thorough risk reviews for new applications and features and obtains the esteemed approval of the Saudi Arabian Monetary Authority (SAMA), ensuring that technology deployments align with the highest regulatory standards
- Actively reviews and approves over 95 application change requests during the initiation stage, which entails robustly navigating the intricacies of GRC (Governance, Risk and Compliance) approvals for essential documents such as Business Requirement Documents (BRD) and Statement of Work (SOW) documents, ensuring that all changes adhere to the established guidelines
- Holds a pivotal position in ensuring the pre-deployment approval process within our information security department. Participates in CAB meetings and provides invaluable insights and rigorous security evaluations for proposed changes
- Manages a significant workload, diligently processed over 3400 requests, spanning diverse categories including firewall configurations, Load Balancer adjustments, IP assignments, hardware requests, copy/cloning operations, VPN setups and critical application changes and ensures that systems remain agile and responsive to the dynamic needs of our organisation
- Oversees and manages the execution of over 950 security scan tasks, utilising our state-of-the-art Archer (eGRC tool). Identifies vulnerabilities but also plays a crucial role in assigning more than 150 observed findings, ensuring that the team can address and rectify these vulnerabilities promptly

Accomplishments:

- Spearheaded risk assessments for over 65 critical applications, proposing strategic controls to enhance system resilience and security, resulting in obtaining approval from SAMA
- Optimised the initiation of more than 95 application changes by effectively navigating the complexities of GRC procedures, ensuring compliance adherence and accelerating deployment processes

Duties and Responsibilities:

- Conducted thorough risk assessments for information systems, applications and processes to meticulously identify potential vulnerabilities and threats, ensuring the security landscape was comprehensively analysed
- Developed multifaceted risk mitigation strategies in close collaboration with cross-functional teams, guaranteeing a comprehensive and well-rounded approach to security that adhered to industry standards and regulatory requirements
- Continuously monitored and systematically reassessed risks, demonstrating the commitment to maintaining a proactive and adaptable risk posture, effectively responding to the ever-evolving threat landscape
- Orchestrated the development, implementation and sustained maintenance of a robust framework of information security policies, procedures and standards. These were meticulously aligned with various regulatory frameworks such as ISO 27001, showcasing a dedication to compliance and best practices
- Conducted internal security audits and in-depth assessments to meticulously evaluate the efficacy of security controls, adeptly identifying areas for enhancement and driving continuous improvement across the security landscape
- Collaborated seamlessly with procurement and legal teams to meticulously assess vendor contracts, ensuring they met stringent security and compliance prerequisites, safeguarding the organisation's interests and information

Accomplishments:

- Collaborated with cross-functional teams to create strategic mitigation plans aligned with industry standards and regulations, ensuring comprehensive risk management
- Managed internal security audits, refining controls and pinpointing opportunities for ongoing enhancement

Duties and Responsibilities:

- Took on the responsibility of configuring security settings for a range of 14 servers, encompassing Linux, Windows, AD, mail servers and alongside this, undertook the task of developing comprehensive information security plans and successfully established more than five robust information security policies
- Was involved in the implementation of Web Application Firewall (WAF), specifically ModSecurity, to enhance the security of our web-based servers. Moreover, effectively configured hardware firewalls such as ASA and StormShield to fortify our defence mechanisms

Information Security Officer, National Ribat University, Continued/....

- Deeply involved in the intricate task of designing secure networks, systems and application architectures. These efforts contributed significantly to maintaining the integrity of our digital infrastructure
- Conducted quarterly vulnerability assessments, leveraging automated tools like Nessus and Nmap. This proactive approach helped identify vulnerabilities and threats that could potentially compromise our systems
- Engaged in manual penetration testing, meticulously evaluating the security posture of our websites and applications. This hands-on testing played a pivotal role in uncovering vulnerabilities that might otherwise have gone undetected
- Encompassed a comprehensive spectrum of security activities, reinforcing the organisation's cybersecurity stance and ensuring the protection of our digital assets

Accomplishments:

- Set up security configurations for more than 14 servers, encompassing Linux, Windows, Active Directory and mail servers, guaranteeing thorough protection
- Enhanced the security of web-based servers by introducing ModSecurity WAF, effectively shielding against a range of online threats

Linux Servers Administrator & Security HostUsZone Sudan

March 2012 - December 2017

Duties and Responsibilities:

- Deployed, configured and maintained Linux server systems to meet the organisation's requirements, which included selecting the appropriate Linux distribution, setting up network parameters and configuring essential services such as 3 new Linux web servers (Apache, PHP, MySQL, CPanel)
- Implemented security measures to safeguard Linux servers against potential threats. This involves applying security patches, configuring firewalls, managing user access and privileges and regularly conducting security audits to identify vulnerabilities
- Continuously monitored server performance, resource utilisation and identified potential bottlenecks. Implemented performance tuning strategies to ensure servers operate efficiently and can handle the organisation's workloads
- Established and managed backup solutions to protect critical data and server configurations. Developed robust recovery procedures to minimise downtime in the event of system failures or data loss
- Managed user accounts, permissions and access control to ensure that users have appropriate levels of access while enforcing security best practices which included enforcing password policies and implementing multi-factor authentication where necessary
- Identified and resolved server-related issues promptly. Troubleshooting hardware and software problems, analysing system logs and working to prevent recurring issues to maintain server stability

Accomplishments:

- Successfully executed the deployment and configuration of Linux servers, incorporating essential services such as Apache, PHP, MySQL and CPanel, customised to meet organisational requirements
- Took a proactive approach to monitor server performance, strategically fine-tuning resources and alleviating bottlenecks to ensure optimal operations

QUALIFICATIONS

- **Bachelor of Science: Computer Science**, University of Gezira

CERTIFICATIONS & PROFESSIONAL DEVELOPMENT

- **Certified in Risk and Information Systems Control (CRISC)**
- **Certified Red Team Professional (CRTP)**
- **EC-Council Certified Security Analyst (ECSA)**
- **Certified Ethical Hacker (CEH)**
- **Red Hat Certified System Administrator (RHCSA)**

LANGUAGES

- **Arabic:** Native
- **English:** Advanced

Azzam Ahmed | Riyadh, Saudi Arabia | +966 509 233 663 | Me@azzamahmed.com | www.azzamahmed.com
