Regional Cybersecurity Advisor

Location: [Africa] [Ghana]

Town/City: Accra

Category: Information Technology

Job Type: Fixed term, Full-time

***Preferred position location: Accra, Ghana. Other possible locations: Dakar, Senegal, Eastern Europe or the Middle East Region where WVI is registered to operate.**

***Please submit your CV in English.**

PURPOSE OF THE POSITION:

Incumbents working in an Regional Cybersecurity Advisor role are responsible for developing and managing security across multiple IT functional areas (e.g., data, systems, network and/or Web) across the enterprise, develop and manage enterprise security services, and develop security solutions for complex assignments to ensure the company's infrastructure and information assets are protected. They work on multiple projects as a team lead.

Individuals within the IT Security job family plan, execute, and manage multi-faceted projects related to compliance management, risk assessment and mitigation, control assurance, business continuity and disaster recovery, and user awareness. They are focused on developing and driving security strategies, policies/standards, ensuring the effectiveness of solutions, and providing security-focused consultative services to the organization.

Individuals develop, execute and manage data, system, network and internet security strategies and solutions within a business area and across the enterprise. They develop security policies and procedures such as user log-on and authentication rules, security breach escalation procedures, security auditing procedures and use of firewalls and encryption routines. To guide enforcement of security policies and procedures, they administer and monitor data security profiles on all platforms by reviewing security violation reports and investigating security exceptions. They update, maintain and document security controls and provide direct support to the business and internal IT groups. IT Security

professionals evaluate and recommend security products, services and/or procedures. They also communicate and educate IT and the business about security policies and industry standards, and provide solutions for enterprise/business security issues.

IT Security professionals require strong technical, analytical, communication and consulting skills with knowledge of IT Security and related technologies. Security certifications (i.e., Certified Information Systems Security Professional (CISSP), Certified in Risk and Information Systems Control (CRISC), Certified Information Security Manage (CISM), Global Information Assurance Certification

(GIAC) and/or other certifications) may be required.

KEY RESPONSIBILITIES:

Strategy:

- Provides strategic and tactical direction and consultation on security and IT compliance.

Policies, Procedures & Standards:

- Maintains an up-to-date understanding of industry best practices.
- Develops, enhances and implements of enterprise-wide security policies, procedures and standards.
- Monitors the legal and regulatory environment for developments.
- Recommends required changes to IT policies and procedures.
- Supports service-level agreements (SLAs) to ensure that security controls are managed and maintained.
- Monitors compliance with security policies, standards, guidelines and procedures.
- Ensures security compliance with legal and regulatory standards.

Business Requirements:

- Engages directly with the business to gather a full understanding of project scope and business requirements.
- Works with customers to identify security requirements using methods that may include risk and business impact assessments.
- Consults with other business and technical staff on potential business impacts of proposed changes to the security environment.
- Provides security-related guidance on business processes.

Security Solutions:

- Works closely with IT and development teams to design secure infrastructure solutions and applications, facilitating the implementation of protective and mitigating controls.

Operations Solutions:

- Defines security configuration and operations standards for security systems and applications, including policy assessment and compliance tools, network security appliances, and host-based security systems.
- Defines and validates baseline security configurations for operating systems, applications, networking and telecommunications equipment.

Risk Assessments:

- Works directly with the customers and other internal departments and organizations to facilitate IT risk analysis and risk management processes and to identify acceptable levels of residual risk.
- Conducts business impact analysis to ensure resources are adequately protected with proper security measures.
- Assesses potential items of risk and opportunities of vulnerability in the network and on information technology infrastructure and applications.
- Reviews risk assessments, analyzes the effectiveness of IT control activities, and reports on them with actionable recommendations.
- Monitors risk mitigation and coordinates policy and controls to ensure that other managers are taking effective remediation steps.
- Manages the oversight of technical risks assessments, such as vulnerability scanning and penetration testing.

Information/Data Security:

- Defines, identifies and classifies information assets.
- Assesses threats and vulnerabilities regarding information assets and recommends the appropriate information security controls and measures.

- Develops and manages security measures for information systems to prevent security breaches.
- Manages project documentation (compliance documentation, security plans, risk assessment, corrective action plans, etc.).
- Consults with clients on the data classification of their resources

Security Audit:

- Performs security audits.
- Participates in security investigations and compliance reviews as requested by external auditors.
- Conducts and reports on internal investigations of possible security violations.
- Consults with clients on security violations.

Security Support:

- Provides security support to ensure that security issues are addressed throughout the project life cycle.
- Provides responsive support for problems found during normal working hours as well as outside normal working hours.
- Leads and responds to security incidents and investigations and targets reviews of suspect areas.
- Consults on teams to resolve issues that are uncovered by various internal and 3rd party monitoring tools.

Business Continuity/Disaster Recovery:

- Coordinates the administration and logistical procedures for disaster recovery testing, and integration of all enterprise “critical” systems.
- Identifies and coordinates resolution of recovery issues.
- Ensures recovery drills are performed and analyzes performance.

Security Performance Management:

- Analyzes reports and makes recommendations for improvements.

Communications/Consulting:

- Serves in an advisory role in application development projects to assess security requirements and controls and ensures that security controls are implemented as planned.
- Collaborates on critical IT projects to ensure that security issues are addressed throughout the project life cycle.
- Informs stakeholders about compliance and security-related issues and activities affecting the assigned area or project.
- Interfaces with business and IT leaders communicating security issues and responding to requests for assistance and information.
- Reports to management concerning residual risk, vulnerabilities and other security exposures, including misuse of information assets and noncompliance.

Vendor Management:

- Works with third party vendors during problem resolutions.
- Interfaces with third party vendors to evaluate new security products or as part of a security assessment process.

Training and Communities of Practice (CoP):

- Develops security awareness and compliance training programs.
- Provides communication and training as needed.
- Provides security briefings to advise on critical issues that may affect client.
- Conducts knowledge transfer training sessions to security operations team upon technology implementation.

Coaching/Mentoring:

- Provides ongoing knowledge transfer to team members and clients on security products and standards.
- Mentors less-experienced team members.

?

KNOWLEDGE, SKILLS AND ABILITIES:

- Bachelor's Degree in Computer Science, Information Systems or other related field, or equivalent work experience.
- Requires in-depth knowledge of security issues, techniques and implications across all existing computer platforms.
- A high proficiency level in specific job related skills is required.
- Must be bilingual. Proficient in English and Spanish languages.
- Typically requires 5 - 7 years of combined IT and security work experience with a broad range of exposure to data protection and privacy, GDPR compliance, PCI-DSS compliance, risk management, incident management, and cybersecurity.
- Experience designing and implementing security solutions.
- Willingness and ability to travel domestically and internationally, as necessary.
- Requires Security Certification (i.e., Certified Information Systems Security Professional (CISSP).
- Effective in written and verbal communication in English (desired).
- Effective in writte and verbal communication in Spanish (preferred).

Preferred Skills, Knowledge and Experience:

- CISSP certification
- PCI-ISA certification
- IAPP-CIPT certification
- Vendor Management experience

- Project Management experience
- Risk Management experience
- Incident Management experience
- Cybersecurity experience
- GDPR experience
- PCI-DSS experience

Work Environment/Travel:

- The position requires ability and willingness to travel domestically and internationally up to 20% of the time.