Zambia Jobs Expertini®

Technical Director, Cybersecurity - Southern Africa

Apply Now

Company: World Vision

Location: Zambia

Category: other-general

With over 70 years of experience, our focus is on helping the most vulnerable children overcome poverty and experience fullness of life. We help children of all backgrounds, even in the most dangerous places, inspired by our Christian faith.

Come join our 33,000+ staff working in nearly 100 countries and share the joy of transforming vulnerable children's life stories!

Key Responsibilities:

PURPOSE OF POSITION:

Individuals working as a Technical Director, Cybersecurity oversee the planning, execution, and management of multi-faceted projects related to compliance, control assurance, risk management, security, and infrastructure/ information asset protection. They are responsible for developing and managing security across multiple IT functional areas (e.g., data, systems, network and/or Web) across the enterprise, developing and managing enterprise security services, and developing security solutions for critical and/or highly complex assignments to ensure the company's infrastructure and information assets are protected. They work on multiple projects or programs as a team lead.

Individuals within the Cybersecurity 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.

IT Security professionals 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.

MAJOR RESPONSIBILITIES:

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

Acts as primary support contact for the development of secure applications and processes.

Maintains an up-to-date understanding of industry best practices.

Develops, enhances and implements enterprise-wide security policies, procedures and standards across multiple platform and application environments. Monitors the legal and regulatory environment for developments. Recommends manages implementation of required changes to IT policies and procedures.

Monitors compliance with security policies, standards, guidelines and procedures.

Ensures security compliance with legal and regulatory standards.

Engages directly with the business to gather a full understanding of project scope and business requirements.

Assesses business needs against security concerns and articulates issues and potential risks to management.

Consults with other business and technical staff on potential business impacts of proposed changes to the security environment.

Provides security-related guidance on business process.

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

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.

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.

Evaluates security risks and identifies and defines compliance strategies in accordance with policies and standards.

Provides management with risk assessments and security briefings to advise them of critical issues that may affect customer, or corporate security objectives.

Communicates with multiple departments and levels of management in order to resolve technical and procedural IT security risks.

Develops remediation strategies to mitigate risks associated with the protection of infrastructure and information assets.

Defines, identifies and classifies information assets.

Assesses threats and vulnerabilities regarding information assets and recommends the appropriate security controls and measures.

Develops and manages security measures for information systems to prevent security breaches.

Consults with clients on the data classification of their resources.

Provides reports to leaders regarding the effectiveness of information security and makes recommendations for the adoption of new policies and procedures.

Develops and implements strategies to align information security with business objectives and goals, protecting the integrity, confidentiality and availability of data.

Performs security audits.

Participates in security investigations and compliance reviews as requested by external auditors.

Consults with clients on security violations.

Acts as liaison between internal audit and IT to ensure commitments are met and controls are properly implemented.

Assists security operations team in troubleshooting and resolving escalated security related issues.

Builds security incident response teams.

Authors incident response plans and support documentation and diagrams.

Develops impact analysis.

Assists business partners with the determination of critical business processes and systems.

Identifies and coordinates resolution of recovery issues.

Develops measures to evaluate the security programs and modifies strategies as appropriate.

Analyzes reports and makes recommendations for improvements.

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.

Provides input for the development of the security architecture.

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.

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.

Coordinates with vendors to ensure managed services are implemented and maintained appropriately.

Leads and reviews application security risk assessments for new or updated internal or third-party applications.

Maintains contact with vendors regarding security system updates and technical support of security products.

Assists in cost-benefit and risk analysis.

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.

Provides ongoing knowledge transfer to team members and clients on security products and standards.

Mentors less-experienced team members.

KNOWLEDGE/QUALIFICATIONS FOR THE ROLE:

Requires 10 - 15 years cyber, privacy, compliance, or risk management function or a closely related role.

Over 10 years of experience as a senior manager or information security officer.

Over 5 years of experience managing cyber security incident response teams. Experience designing and implementing security solutions.

Requires in-depth knowledge of PCI-DSS, privacy laws, security standards, security best practices, and security regulations. A high proficiency level in threat management, risk management, vulnerability management, and compliance management is required.

Effective in written and verbal communication in English

Willingness and ability to travel domestically and internationally, as necessary.

Bachelor’s degree in Computer Science, Information Systems or other related field, or equivalent work experience.

Requires Security Certification (i.e., Certified Information Systems Security Professional (CISSP), Certified Information Security Manage (CISM), or Global Information Assurance Certification (GIAC).

Fluent in English.

Have strong incident and investigation management skills.

Have strong communication skills.

Have good planning and organising skills.

Strategic thinker with strong influencing skills and exceptional professional credibility.

Outstanding stakeholder management skills combined with the ability to challenge and influence in a constructive manner.

Have proven ability to collaborate effectively and develop positive working relationships across all levels of an organisation.

Have strong analytical skills, with the ability to gather, analyse and evaluate information and to prepare concise written reports.

Have technical expertise on risk assessment tools and methods or the willingness to learn.

Good understanding of the different field contexts or experience working in at least 2 different contexts (e.g. development, transitioning, fragile, conflict, humanitarian, etc.)

Apply Now

Cross References and Citations:

1. **Technical Director, Cybersecurity - Southern Africa Jobs Zambia ↗**
2. **Technical Director, Cybersecurity - Southern Africa Jobs Zambia ↗**
3. **Technical Director, Cybersecurity - Southern Africa Jobs Zambia ↗**
4. **Technical Director, Cybersecurity - Southern Africa Jobs Zambia ↗**
5. **Technical Director, Cybersecurity - Southern Africa Jobs Zambia ↗**
6. **Technical Director, Cybersecurity - Southern Africa search Zambia ↗**
7. **Technical Director, Cybersecurity - Southern Africa job finder Zambia ↗**

1. **Technical Director, Cybersecurity - Southern Africa jobs↗**
2. **Technical Director, Cybersecurity - Southern Africa jobs↗**
3. **Technical Director, Cybersecurity - Southern Africa jobs↗**