Internal/External Vacancy Advert

Date of advertisement: 06 September 2021

About us:

Our commitment to our stakeholders is to be the best and most successful IT distributor in our region. We strive towards this goal by being the most valued channel for our partners and by contributing to the growth and profitability of our shareholders, staff, vendors, channel partners and their customers.

Axiz is an equal opportunity employer and this position will be filled in accordance with our current Employment Equity practices.

Job Specification:

Position:	Information Security Manager	**Location:**	Gauteng
Company:	Axiz	**Department:**	Advanced Technologies – Security
Employment Type:	Permanent	**Reporting to:**	Security Business Unit Manager

Purpose of the position:

The role of the Information Security Manager will be to provide sound technical leadership and facilitating the development of an information security practice for Axiz customers. You will be the one to devise the security strategy and ensure that all systems necessary to support operations and objectives are in place. You will oversee the technical responsibilities of the security /services team, engaging SOC management and collaborate with Vendors daily. Strategic thinking, leadership and strong business acumen are essential in this role. You're expected to be well-versed in current security technological trends, familiar with a variety of business concepts and be hands on. The goal is to ensure that Axiz adds the maximum value to the customers security strategy.

Key Responsibilities:

Information Security Practice Development:

- Ensure the development of Information Security architectures (considering people, information, processes and technology). Key understanding of building zero-trust architectures/secure access service edge for our customers, driving adoption through consulting C-level executives and implementing strategies to drive security managed services through our SOC platform going forward.
- Develop and maintain plans to implement the Information Security strategy and ensuring alignment with others in the organization. This will include training our staff and changing the velocify on how Axiz approach our customers.
- Specify the activities to be performed within the Information Security program / projects.
- Develop a program for Information Security awareness, training and education.
- Recommend and advise Information Security requirements into the customers processes and lifecycle activities (e.g., change control, software development, employment, procurement etc.).
- Establish metrics to evaluate the effectiveness of the Information Security program.
- Establish, communicate and maintain Information Security policies, standards, procedures and other documentation that support Information Security architectures.
- Develop MSP programs based on Tier one Vendor strategies. Align those programs with SOC services (Advanced Technology Services) and building Axiz managed security services out.
- Developing and implementing processes for preventing, detecting, identifying, analyzing and responding to information security incidents.
- Establish reporting and communication channels that support Information Security.
- Developing a process to communicate with internal and external stakeholders.

Information Security Program Management:

- Oversee the execution of Information Security programs.
- Oversee the performance of contractually agreed information security controls (e.g., with joint ventures, outsourced providers, business partners, third parties).
- Provide Information Security advice and guidance (e.g., risk analysis, control selection) across customer base.
- Provide Information Security awareness, training and education to stakeholders (e.g., business process owners).
- Monitor, measure and report on the effectiveness and efficiency of Information Security controls and compliance with Information Security policies. Alignment with SLA manager in the SOC team would be crucial to highlight improvement and identify risks that need to be mitigated.

Information Security Incident Management and Response:

- Develop and maintain plans to respond to and document Information Security incidents.
- Develop and implement processes for preventing, detecting, identifying, analysing and responding to Information Security incidents. Working with SOC team and

Information Security Governance/Risk management:

- Identifying current and potential legal and regulatory requirements for our customers. Axiz customers cover all verticals, understanding compliance requirements is critical.
- Establish a process for information asset classification and ownership.
- Implement a structured information risk assessment mitigation and reporting process.
- Ensure that threat and vulnerability evaluations are performed on an ongoing basis to show customers value distinction in the market.
- Identify and periodically evaluate Information Security controls and countermeasures to mitigate risk to acceptable levels.
- Integrate risk, threat and vulnerability identification and management into operational management and program delivery processes.
- Ensuring the development of information security architectures. Customer's security maturity levels differ. A roadmap on where each customer is going is key to success. Building blocks highlighting improvement on their security journey with Axiz will show customer stakeholders investment they made with Axiz.
- Developing a program for information security awareness, training and education.
- Recommend and advise information security requirements.
- Overseeing the execution of information security programs and the performance of contractually agreed information security controls getting processes in place to mitigate risk as well as methodical steps taken to help with incident response. Process around malware analysis/threat hunting.
- Establish escalation and communication processes and lines of authority.
- Track and facilitate the investigation of Information Security incidents (e.g., forensics, evidence collection and preservation, log analysis, interviewing).
- Develop a process to communicate with internal and external stakeholders.
- Integrate Information Security incident response plans with the customers disaster recovery and business continuity plan.
- Formulate training and awareness programs for Information Security incident response.
- Provide guidance on the resolution of major Information Security incidents.
- Facilitate reviews to identify root causes of Information Security incidents, facilitate corrective actions and re-assess risk.

Job Requirements:

Education and Experience:	• Bachelor's degree in Computer Science or Information Systems or equivalent qualification • CISSP certification (Certified Information Systems Security Professional) • CISM certification (Certified Information Security Manager) • Accredited certification in Problem Management (e.g.ITIL intermediate course) • Accredited IT Risk Management certification • Accredited certification in Project Management (e.g. PMP, Prince2) • COBIT-5 certification in IT Governance • 7-10 years relevant Information Security (InfoSec) Management experience in an enterprise environment. • IT Service Management experience is advantageous • Proficiency in legal, regulatory and other compliance requirements related to InfoSec (e.g. POPIA).
Technical Competencies:	• Developing and managing InfoSec projects / programs. • Security incident management, Security Investigations and root cause analysis. • Developing InfoSec policies, plans and procedures aligned to ISO 27001 & 27002 standards. • Advanced proficiency in MS Office
Behavioural Competencies:	• Excellent English Communication skills (verbal and written) • Strong facilitation and interpersonal skills • Excellent planning, coordination and time management skills • Strong business acumen

Application Process:

Contact Person: The Recruitment Team

Telephone Number: 011 237 7000

E-mail address: careers@axiz.com

Closing Date: 13 September 2021

The company is under no obligation to fill this position and should you not have had any feedback within 2 weeks after the closing date, you may consider your application unsuccessful.