African Rainbow Minerals

CAREER OPPORTUNITY

African Rainbow Minerals is a leading South African diversified mining and minerals company, with world-class long-life, low unit cost assets. We offer opportunities for career advancement, development and retention. Our **"WE DO IT BETTER"** philosophy has positioned us to be an Employer of Choice.

Applications are invited from suitably qualified and experienced persons for the position of **Information Security Specialist**, reporting to the Chief Information Officer. The position will be based in Sandton, Johannesburg.

Information Security Specialist

(D-Upper Patterson grading)

Purpose of the Job:

- Set direction and rules for enterprise-wide management Information Security Risk, measure outcomes and direct the applicable management action.

Job Requirements:

- IT/IS related Honours Degree (Essential/Minimum).
- BSc (Honours) Information Systems Technology / BComm (Honours) Informatics.
- Information Security Certifications - CISSP, CISM, CEH, etc. (recommended/desirable).
- Certified Risk and Information Systems Control (CRISC) - ISACA (recommended/desirable).
- Broad and in-depth knowledge & skills, with the ability to deal with exceptions and special cases in an independent manner on:
  - IM Infrastructure;
  - Managing complexity;
  - IM Project delivery & methodology;
  - Professional skills;
  - Information Security applications and methods.

- Good working knowledge of:
  - Technology services & operations;
  - IT service management and customer services;
  - Business/Client management;
  - Business acumen;
  - Leadership & management;
  - Planning & management.

Job Responsibilities:

Information Security Management:

- Identify and prioritize enterprise level Information Security threats and risks.
- Manage the baseline minimum standard for Information Security controls, aligned to industry standards, legal and regulatory requirements.
- Maintain and enforce Information Security policies and non-technical standards.
- Manage the risks associated with exceptions to Information Security policy and standards.
- Manage trends and assets by which Information Security accountability and controls are instantiated across the environment.
- Maintain effective relations with relevant stakeholders.
- Manage metrics program to give quantitative insight into security posture.
- Review the overall effectiveness of the environment.
- Identify and track improvement opportunities for the security landscape.
- Manage the certification of baseline standards for relevant sections in the organization.
- Manage strategic projects to improve governance and risk management capability.
- Plan and manage complex deployment of security related activities.
- Identification and reporting on suspected breaches and review findings with key stakeholders.
- Establishment of application and infrastructure security control mechanisms.
- Security training awareness, creating material, and sending communications to ensure the users are sufficiently knowledgeable around threats and how to mitigate such threats.
- Ensure all reports and operations of security tools are providing sufficient coverage, and providing the necessary outcomes.
- Ensure there is an effective Patch Management Policy/Standard in place, and has the appropriate security controls.
- Ensure to escalate all issues and concerns.
- Ensure security and risk is a required consideration for projects.

Information Security Administration:

- Verify the adequacy of security controls of applications, cloud, infrastructure, and/or service providers through a standardized assessment work plan customized based on the specifics risks of the target.
- Monitor systems and solve problems; interact and support relationships with administrative and enforcement agencies as necessary.
- Manage and/or participate in deployment of security related activities.
- Assist in development of the Information Security Assessment plan.
- Identify, recommend, and report improvements to IM processes and controls.
- Ensuring efficient user & access management as per access profile.
- Enforcement of security policies and procedures across data centre, networks, databases and applications.

- Assist and train other assessment staff in the use of computerized assessment techniques, and in developing methods for review and analysis of computerized information systems.
- Keep abreast of company policies and procedures, current developments in security and privacy, and related changes in local, state, and federal law.
- Ensure up-to-date policies, standards and procedures to ensure demonstrable regulatory, legal control.

Business Continuity Management:

- Collaborate with service providers to develop business continuity plans (BCP).
- Utilize effective communication channels and training to understand accountability for effective and efficient plan maintenance as part of the overall governance priorities.
- Provides business continuity expertise to relevant stakeholders.
- Maintains all documentation and processes required.
- Align all new IM products and services to the BCP.
- Performs all required audits and tests related to the BCP.
- Participating in/leading special projects as needed.
- Lead the effort to create leveraged solutions and support groups to reduce the overall footprint of standalone dedicated solutions.
- Support implementation of Business Continuity Management (BCM) across business and functions as per the enterprise BCM policy and mandated process and templates.
- Support the development of tools, templates, process, methodology and standardization for BCM and ensure that it is relevant and compliant with the industry standards.
- Act as a subject matter expert and provide support and guidance in development of BCMS plans.
- Coordinate, analyze and report various operational metrics on progress and compliance of BCM plans with proper governance from business/functional/geographic leadership.
- Support the BCM incident management and monitor lesson learned implementation, including simulation exercises.
- Coordinate responses to the non-standard requirements in various products or services, where required.
- Ensure compliance through ongoing audit and sample reviews.
- Support audits externally or internally for the BCM requirements.

Risk Management:

- Participate in company risk initiatives and provide inputs for the risk assessment process.
- Conduct or participate in reviews to assess the service delivery control environment and evaluate adherence to business identified requirements, enterprise policies and standards.
- Ensure that identified findings and actions are tracked to closure and reported to relevant stakeholders.
- Facilitate sharing of learning from matters requiring interventions, such as incidents, initiate process improvements and updates to policies and standards.

- Interact with other enterprise functions, including Internal Audit, Information Security, Risk and Quality Management/Quality Assurance, Legal/Contract Management, Policy teams, IM delivery teams and business groups to ensure the risk management process is efficient and effective.
- Participate and contribute to risk management status reporting and planning with relevant stakeholders.
- Control of assurance monitoring and tracking, including the retention of adequate records.
- Scheduling risk, security and compliance audits, review the outcomes of the audit process.
- Follow up with the relevant stakeholders with regards to audit findings.
- Directing compliance issues to appropriate resources for investigation and resolution.

Compliance, Governance and Assurance:

- Adhere to the all corporate governance, processes, procedures, statuary, legal and other requirements.
- Support the organisational culture and values.
- Entrench a culture of discipline and transparency.

Safety & Health:

- Maintain and ensure a healthy environment, safe operational practices, ensuring compliance with all applicable SHERQ policies procedures in line with set standards.
- Encourage a culture that focuses on safety in all operations.

Personal Attributes:

- Professional;
- Reliable;
- Transparent;
- Ability to work under pressure;
- Resilience;
- Innovation and taking initiative;
- Teamwork and cooperation;
- Advanced problem solving;
- Effective communication;
- Self-leadership and discipline;
- Listening, interpretation and communication;
- Conflict management.

Interested applicants are invited to e-mail their CVs to ARM Recruitment, by no later than **22 December 2020**.

Email: recruitment@arm.co.za

Equity Statement:

Preference will be given to suitably qualified Applicants from designated groups in line with the Employment Equity Plan and Targets of the Organisation.

NOTE: If you are not contacted within 21 days after the closing date, please consider your application to be unsuccessful.