VACANCY NOTICE

Applications are invited from suitably qualified persons to fill the following posts within the Zimbabwe Revenue Authority (ZIMRA) – an equal opportunity employer.

1. SENIOR ICT RISK MANAGER, CORPORATE COMPLIANCE & RISK – LEVEL 6 (1 POST)

1.1 Key Responsibilities

- Provides strategic advisory services to Business and ICT on emerging technologies, digital innovation and evolving cyber threats affecting the Authority,
- Interprets and translates international ICT risk, security and data protection standards into Authority-wide governance requirements.
- Evaluates Authority-wide ICT investments to assess risk exposure, value realization, and alignment with strategic objectives.
- Assesses ICT project risks from initiation through implementation and post-go-live stages.
- Reviews and validates Business Continuity Plans, BIAs, and ICT Disaster Recovery Plans.
- Provides governance oversight during disaster recovery simulations and incident response testing.
- Monitors system changes and verify replication between primary and DR environments.
- Provides strategic oversight of the ICT Risk Register.
- Prioritises ICT risks based on enterprise impact and risk appetite.
- Assesses Authority systems for security vulnerabilities and control weaknesses.
- Reviews access management, authentication, and logging controls.
- Evaluates communication security and data leakage risks
- Assesses data protection maturity of vendors.
- Reviews data processing agreements
- Provides enterprise-wide oversight of compliance with data protection legislation.
- Monitors adherence to Cyber & Data Protection Act and SI 155 of 2024.
- Embeds data protection requirements into ICT and business processes.
- Advises senior management on privacy risks and mitigation strategies
- Identifies high-risk data processing activities.
- Facilitates privacy risk analysis with stakeholders.
- Recommends safeguards and mitigation measures.
- Tracks implementation of DPIA actions.

1.2 Job Skills and Competencies

- Ability to work under pressure,
- Ability to communicate at all levels,
- Ability to work both independently and as part of a team,
- Unquestionable integrity,
- Computer literacy

1.3 Qualifications and Experience

- Bachelor's Degree in Information Technology, Information Systems, Computer Science, Information Security, Risk Management, or a related field is a must.
- Postgraduate qualification in Information Systems Management, Computer Science, Risk Management is a must
- At least eight (8) years postgraduate experience in ICT / Risk Management
- Certified Data Protection Officer Certification (POTRAZ) is a must
- Professional certification in ICT Risk, Information Security, or Governance, such as: CRISC, CISM, or CISA, ISO / IEC 27001 Lead Implementer or Lead Auditor ISO / IEC 27701 Lead Implementer / Auditor or COBIT Foundation / Design and Implementation is a must
- Experience in Customs / Domestic Taxes or Tax environment is an added advantage.
- A thorough understanding of risk management practices is a must

2. DATA PROTECTION SPECIALIST, CORPORATE RISK & COMPLIANCE – LEVEL 8 (1 POST)

2.1 Key Responsibilities

- Implements and operationalises the Authority's data protection governance framework across all systems, applications, and business processes, ensuring alignment with statutory and policy requirements
- Develops, maintains, and validates Records of Processing Activities (RoPA) across all ZIMRA functions, ensuring completeness and accuracy of processing records.
- Identifies high-risk personal data processing activities and facilitate Data Protection Impact
- Assesses (DPIAs) in collaboration with business, ICT, Legal, and security teams.
- Coordinates handling of data subject rights requests including access, correction, deletion, objection, restriction, and monitor compliance with statutory timelines.
- Conducts periodic data protection compliance reviews across business units and ICT systems and monitor implementation of corrective actions.
- Supports coordination of data breach and incident response activities, including impact assessment preparation of regulatory notification documentation.
- Supports engagement with the Data Protection Authority (POTRAZ) and prepare compliance documentation for inspections, enquiries, and regulatory reviews.
- Assesses data protection maturity of third-party vendors and processors and monitor remediation of identified compliance gaps.
- Reviews new systems, projects, and process changes to ensure privacy-by-design principles are applied and privacy risks are addressed at design stage.
- Identifies and document data protection risks and maintain privacy risk and issue registers to support enterprise risk reporting.
- Supports development and delivery of data protection awareness and training programmes and evaluate effectiveness of initiatives.
- Supports internal and external audits relating to data protection and privacy and track closure of audit findings.
- Conducts any other duties as may be assigned.

2.2 Job Skills and Competencies

- Self-starter with the ability to work under pressure and beyond stipulated hours.

- Unquestionable integrity and commitment to duty.
- Good analytical skills.
- Ability to interact with various departments such as Legal Compliance, Audit and internal and external stakeholders in Information Technology.
- Good communication and interpersonal skills.
- Good organisational, people and time management skills.

2.3 Qualifications and Experience

- Bachelor's degree in information systems, Computer Science, Risk Management, Data Science, Information Management, Law, Business Studies or a related field is a must
- A Postgraduate degree in Information Technology, Risk Management, Data Analytics, or related fields is an added advantage.
- Certified Data Protection Officer (POTRAZ) certification is a must.
- Certification in ICT Governance, Risk or Security such as CRISC, CISM, CISA, CISSP, COBIT or ISO / IEC 27001 Lead Implementer / Lead Auditor or equivalent is a must.
- At least five (5) years postgraduate experience in data privacy / protection.
- Experience in Customs / Domestic Taxes or Tax environment is an added advantage.

3. ICT SECURITY GOVERNANCE SPECIALIST, CORPORATE RISK & COMPLIANCE – LEVEL 8 (1 POST)

3.1 Key Responsibilities

- Implements and operationalises the Authority's information security governance framework across all ICT systems, applications, infrastructure, and data platforms.
- Translates approved security policies, standards, and frameworks into system-level security control requirements.
- Coordinates consistent application of security controls across ICT domains and business units.
- Monitors adherence to information security policies and escalate non-compliance.
- Reviews security controls implemented within core and supporting systems (e.g. ERP, customs, revenue, analytics platforms).
- Assesses security architecture, configuration, and integration controls at application and database level.
- Identifies systemic and recurring security control weaknesses across systems.
- Supports governance reviews for new systems, upgrades, and system integrations
- Reviews access control models, user provisioning processes, and segregation of duties across systems.
- Conducts periodic security control assessments in line with approved assurance plans.
- Coordinates vulnerability assessment and penetration testing activities from a governance perspective.
- Assesses security risks arising from ICT change initiatives and digital transformation projects.
- Assesses security controls implemented by ICT vendors, cloud providers, and service partners.
- Reviews compliance with contractual and regulatory security requirements.
- Monitors remediation of third-party security gaps.
- Identifies and documents information security risks across systems and processes.

- Maintains accurate and up-to-date security risk and issue logs.
- Supports implementation and review of information security policies and standards.
- Contributes to cybersecurity awareness and training initiatives
- Supports internal and external audits relating to information security governance.
- Tracks and monitors closure of security-related audit findings.
- Provides assurance inputs to support executive and Board reporting.

3.2 Job Skills and Competencies

- Ability to work under pressure,
- Ability to communicate at all levels,
- Ability to work both independently and as part of a team,
- Unquestionable integrity,
- Computer literacy.

3.3 Qualifications and Experience

- Bachelor's degree in information security, Information Technology, Information Systems, Computer Science, Cybersecurity, Finance, Business Management or a related field.
- Postgraduate qualification in Information Security, Cybersecurity, Data Analytics, Risk Management, or ICT Governance is an added advantage.
- Professional certification in Information Security or ICT Governance such as: CISM, CISSP, ISO / IEC 27001 Lead Implementer or Lead Auditor, COBIT is a must.
- At least five (5) years of postgraduate experience in an ICT / Risk Management environment.
- Training or certification in ICT risk or cybersecurity governance (added advantage)
- Experience in Customs / Domestic Taxes or Tax environment is an added advantage.

4. CORPORATE COMPLIANCE SUPERVISOR, CORPORATE RISK & COMPLIANCE – LEVEL 9 (1 POST)

4.1 Key Responsibilities

- Implements and maintains the Authority's compliance management policies and procedures.
- Implements and manages an effective legal compliance programme.
- Conducts compliance gap analysis and providing timely advice and support for legal compliance issues.
- Provides guidance on the proper application and interpretation of laws and regulations affecting compliance of the operations of the Authority.
- Contributes to the effective management of legal and compliance risks.
- Ensures proactive and timely monitoring, identification dissemination and advice on compliance and regulatory developments, changes and practices associated risks.
- Ensures adequacy of controls to mitigate legal compliance risks and roll out compliance policies and procedures.
- Establishes and maintaining effective processes, including training, advice and support, to ensure that compliance policies, procedures and standards are timeously and effectively implemented.
- Implements a Compliance Monitoring Programme and ensure timely conduct of compliance assessment / reviews.

- Prepares and maintains a compliance tracking log.

4.2 Job Skills and Competencies

- Self-starter with the ability to work under pressure and beyond stipulated hours.
- Unquestionable integrity and commitment to duty.
- Ability to work during odd hours in an area with poor road terrain and bad weather conditions.
- Good analytical skills.
- Ability to interact with various departments such as Legal Compliance, Audit and internal and external stakeholders in Information Technology.
- Good communication and interpersonal skills.
- Good organisational, people and time management skills.

4.3 Qualifications and Experience

- A Bachelor's degree in Law / Risk Management / Business Studies / Fiscal Studies / ICT / Accounting or equivalent.
- At least three (3) years' relevant post graduate experience in Enterprise Compliance, Legal, Governance or Risk Management.
- Experience in Customs / Domestic Taxes or Tax environment is an added advantage.
- A professional qualification in Compliance & Governance Certification / Risk Management Certification is an added advantage.
- An MBA / MSc or equivalent is an added advantage.

Interested candidates should submit applications, accompanied by a detailed Curriculum Vitae by **28 March 2026**, All applications should be emailed to: ZimraRecruitment@zimra.co.zw **clearly** stating the position applied for and addressed to:

The Director, Human Capital
Zimbabwe Revenue Authority
6th Floor ZB Centre
Corner First Street / Kwame Nkrumah Avenue
P. O. Box 4360
HARARE

Please note that only shortlisted applicants will be responded to and females are encouraged to apply.