VACANCY NOTICE

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

HEAD ICT OPERATIONS & SERVICE DELIVERY – ICT - LEVEL 5 (1 POST)

Job Purpose

Provide strategic leadership and oversight of ICT Operations and Service Delivery across the Authority, ensuring resilient, secure and efficient enterprise and taxpayer-facing systems. The role leads ICT support operations, service management, governance and nationwide service delivery in alignment with ZIMRA's strategic and digital transformation objectives, reporting to the ICT Director.

Key Responsibilities

- Provide strategic leadership for ICT Operations and Service Delivery across the Authority.
- Develop and implement ICT service delivery strategies, operational frameworks, standards and policies aligned to organisational objectives.
- Ensure effective governance, performance management, operational resilience and continuous improvement of ICT services.
- Drive ICT operational excellence and support the Authority's digital transformation initiatives.
- Oversee enterprise-wide operational support services for Customs, Domestic Taxes, ERP and other corporate systems.
- Ensure high availability, reliability, performance and optimisation of mission-critical taxpayer-facing and enterprise platforms.
- Direct incident, problem, change and service request management processes in line with ITIL best practices.
- Ensure effective management and support of core enterprise, revenue, compliance, human capital and operational systems, including ASYCUDA, Single Window, ECTS, TaRMS, FDMS, SAP ERP and other strategic platforms.

- Implement and maintain ICT governance controls, operational standards, audit requirements and compliance frameworks aligned to COBIT, ITIL, ISO/IEC 27001, NIST and applicable ICT policies.
- Ensure operational risk management, business continuity, cybersecurity compliance and disaster recovery preparedness.
- Maintain audit-ready operational documentation, governance artefacts, technical standards, compliance evidence and operational dashboards.
- Conduct root cause analysis, service reviews and continuous service improvement initiatives.
- Collaborate with business units, vendors, regulators, financial institutions and multidisciplinary ICT teams to enhance enterprise service delivery.
- Manage service level agreements (SLAs), vendor performance, operational reporting and stakeholder engagement processes.
- Ensure delivery of high-quality customer-focused ICT services across the Authority.
- Lead, mentor and develop managers, specialists, analysts, graduate trainees and technical support teams.
- Promote knowledge sharing, innovation, teamwork and a culture of continuous improvement.
- Manage team performance and ensure effective utilisation of ICT operational resources.

Job Skills and Competencies

- Strong leadership and people management capability.
- Ability to lead enterprise ICT support operations and service delivery teams nationwide.
- Strong understanding of enterprise ICT governance, cybersecurity, digital transformation and tax administration environments.
- Sound knowledge of enterprise governance frameworks including COBIT 2019, ITIL 4, ISO/IEC 27001, NIST CSF, GDPR and data protection legislation.
- Strong analytical, troubleshooting, operational risk management and problem-solving skills.
- Ability to work effectively in multidisciplinary, high-pressure and mission-critical environments.
- Excellent communication, stakeholder engagement, technical reporting and presentation skills.
- Strong understanding of enterprise systems integration, operational resilience, audit readiness and compliance management.

- Ability to drive service excellence, operational efficiency and continuous improvement initiatives.
- Strong strategic planning, decision-making and organisational skills.

Qualifications and Experience

- Bachelor's Degree in ICT, Computer Science, Information Systems, or an equivalent discipline.
- ITIL Certification or equivalent is mandatory.
- Relevant ICT Service Management certification will be an added advantage.
- Relevant professional certifications aligned to enterprise ICT governance and operations such as COBIT, ISO/IEC 27001, CISSP, PMP, or related certifications will be an added advantage.
- Minimum of eight (8) years' relevant ICT experience, including significant exposure to enterprise ICT operations, service delivery, or systems support leadership.
- Proven experience supporting large-scale enterprise platforms, taxpayer-facing systems, or public sector digital transformation initiatives.
- Solid exposure to ICT service management environments and ITIL-compliant service desk solutions such as ManageEngine or equivalent platforms.
- Experience in public sector, revenue administration, or other highly regulated environments will be an added advantage.

BUSINESS RELATIONSHIP MANAGER – ICT - LEVEL 7 (1 POST)

Key Responsibilities

- Align ICT initiatives with enterprise strategy and validate business requirements.
- Oversee ICT project portfolio prioritisation, planning and resource allocation.
- Supervise Business Systems Analysts and Business Process Improvement Analysts.
- Coordinate stakeholder engagement and ensure effective communication between ICT and business units.
- Ensure compliance with governance frameworks, audit requirements and regulatory standards.
- Oversee risk management, quality assurance and continuous improvement across ICT projects.
- Lead change management initiatives to support the adoption of ICT systems.
- Monitor ICT vendor performance, manage contracts and ensure SLA compliance.

- Ensure proper documentation of requirements, processes and governance artefacts.
- Support digital transformation initiatives by aligning systems and business processes.
- Mentor graduate trainees, junior analysts and technical teams while promoting knowledge sharing and continuous improvement.

Job Skills and Competencies

- Ability to align ICT initiatives with organisational strategy and drive business-focused digital transformation.
- Strong knowledge of ICT governance, regulatory compliance, audit requirements and risk management frameworks.
- Proven capability to oversee ICT project portfolios, prioritise initiatives and manage resources effectively.
- Skilled in business requirements analysis, process optimisation and the implementation of efficient business solutions.
- Excellent communication and stakeholder engagement skills with the ability to build strong ICT-business relationships.
- Demonstrated leadership experience in supervising teams, driving performance and fostering continuous improvement.
- Ability to manage ICT project risks, ensure quality standards and support governance best practices.
- Proven ability to lead change management initiatives and support successful adoption of ICT systems.
- Experience in managing ICT vendors, contracts and service level agreements to ensure optimal service delivery.
- Strong understanding of enterprise ICT systems, emerging technologies and digital transformation initiatives.
- Strong knowledge of ICT governance frameworks (COBIT 2019, ITIL, ISO standards)
- Strong analytical, problem-solving, troubleshooting and operational risk management capability.
- Ability to work effectively in multidisciplinary, high-pressure and mission-critical environments.
- Excellent communication, stakeholder engagement, technical reporting and presentation skills.
- Ability to manage priorities, support operational excellence and drive continuous improvement initiatives.

Qualifications and Experience

- Bachelor's Degree in Computer Science, Information Systems, Business Studies, or related discipline
- Minimum 5+ years' experience in ICT and business environments.
- At least 3 years leading Business Relationship Management.
- At least one relevant professional certification aligned to the role specialisation and enterprise ICT governance requirements. (Certified Business Relationship Manager (CBRM) Project Management Professional (PMP) / PRINCE2 Practitioner, ITIL Certification2, COBIT 2019 Certification and any other relevant professional certification.)

PROJECT MANAGER – ICT – LEVEL 7 (2 POSTS)

Key Responsibilities

- Lead and support enterprise ICT and digital transformation initiatives aligned to ZIMRA strategic objectives and modern tax administration requirements.
- Lead the planning, execution, monitoring and closure of ICT projects and programmes.
- Develop and maintain key project management artefacts, project plans, budgets, risk registers, issue logs and benefits realisation reports.
- Define project scope, validate functional and technical requirements and oversee feasibility assessments.
- Manage stakeholder engagement, ensuring alignment between ICT initiatives and business strategy.
- Monitor project budgets and expenditures, ensuring adherence to approved financial allocations.
- Identify, assess and mitigate project risks; escalate enterprise-level risks where required.
- Enforce quality assurance standards and ensure compliance with governance, audit and regulatory requirements.
- Lead organisational change management initiatives to support the successful adoption of new systems.
- Prepare executive-level reports for Project Boards, Steering Committees and ICT leadership.
- Ensure projects contribute to digital transformation objectives, revenue enhancement, operational efficiency and stakeholder satisfaction.

- Implement governance controls, operational standards, audit requirements and compliance frameworks such as COBIT, ITIL, ISO/IEC 27001, NIST and ICT policy.
- Mentor graduate trainees, junior analysts and technical teams while promoting knowledge sharing and continuous improvement.

Job Skills and Competencies

- Strong understanding of enterprise ICT governance, cybersecurity, digital transformation and tax administration environments.
- Knowledge of enterprise governance frameworks including COBIT 2019, ITIL 4, ISO/IEC 27001, NIST CSF, GDPR and data protection legislation.
- Strong analytical, problem-solving, troubleshooting and operational risk management capability.
- Ability to work effectively in multidisciplinary, high-pressure and mission-critical environments.
- Excellent communication, stakeholder engagement, technical reporting and presentation skills.
- Strong understanding of enterprise systems integration, operational resilience, audit readiness and compliance management.
- Ability to manage priorities, support operational excellence and drive continuous improvement initiatives.

Qualifications and Experience

- Bachelor's Degree in Computer Science, Information Systems, Business Studies, or related discipline
- Minimum 5+ years' experience in ICT and business environments.
- At least 3 years leading enterprise-scale ICT projects.
- Demonstrated experience in stakeholder management, project governance and benefit Realisation.
- PMP (Project Management Professional) or PRINCE2 Practitioner, Agile Certification (e.g., PMI-ACP, Scrum Master) or any Project Management Certification

SECURITY ARCHITECTURE MANAGER – ICT – LEVEL 7 (1 POST)

Key Responsibilities

- Direct and oversee containment, eradication and recovery actions for escalated incidents across network, application and database domains

- Ensure architecture standards are enforced, monitoring services meet requirements and forensic evidence from incidents is preserved
- Oversee documentation of architecture controls, validate compliance artefacts and ensure regulatory and audit standards are met
- Review systemic threats across all security domains, approve mitigation strategies and escalate risks to Head of Cyber Security
- Approve inventories of enterprise assets (network, applications, databases), validate patch schedules and ensure secure configurations are maintained
- Chair post-incident reviews, approve updates to architecture playbooks and ensure lessons learned are institutionalized across the division
- Enforce architecture standards, lead peer review processes and embed continuous improvement across all security domains
- Supervise Specialists (Network, Applications & Database Security); provide mentoring, performance feedback and ensure skills development plans are executed
- Participate in cybersecurity drills, red team/blue team exercises and disaster recovery simulations; benchmark architecture governance against best practice.
- Any other duties as may be assigned by the Head of Cybersecurity

Job Skills and Competencies

- Demonstrated exposure to systemic risk escalations, compliance audits, enterprise resilience planning and architecture validation across network, application and database domains.
- Experience leading multi-disciplinary teams (IT, Risk, Audit, Compliance, Legal, CERTs) to ensure coordinated governance alignment.
- Understanding of common security standards: ISO 27001, COBIT, NIST; compliance with Zimbabwe's Data Protection and Cyber Security Act.
- Self-starter with ability to work under pressure, including in 24/7 monitoring environments
- Proven decision-making ability under pressure.
- Strong communication and presentation skills along with the ability to work in a highly collaborative environment

Qualifications and Experience

- A graduate Degree in Computer Science or Information & Communication Technology or equivalent qualification.

- A Postgraduate qualification in Master's in Information Security, Cyber Security, Risk Management, or ICT Governance) is an added advantage.
- Must have at least one of the following certifications: CISM (Certified Information Security Manager); CISSP (Certified Information Systems Security Professional); COBIT 2019 Foundation or Practitioner; ISO/IEC 27001 Lead Implementer or Lead Auditor; or a comparable security certification.
- Minimum of five (5) year experience in ICT of which three (3) years should be in ICT security, or equivalent experience in areas such as ICT Risk Management or ICT Audit

SYSTEMS DEVELOPMENT MANAGER, TAXES – ICT – LEVEL 7 (1 POST)

Key Responsibilities

- Lead the design, development, testing and deployment of secure, scalable tax systems (i.e.. TaRMS, FDMS etc).
- Oversee system changes, ensuring proper governance, documentation and compliance with change management processes.
- Promote knowledge management by ensuring accurate documentation, shared repositories and continuous learning within development teams.
- Drive innovation through new system enhancements, including modern technologies (e.g., blockchain, AI).
- Enforce coding standards, quality assurance practices and continuous improvement across all teams.
- Ensure compliance with regulatory, security and data protection standards (e.g., ISO/IEC 27001, Tax Laws).
- Manage risks, internal controls and system integrity, including configuration and version control.
- Direct project execution, ensuring timely delivery and alignment with business requirements.
- Oversee incident and service request management, including monitoring trends and improving system performance.
- Lead organizational change initiatives and ensure adoption of new processes and technologies.
- Mentor and develop multidisciplinary teams (TaRMS Developers and FDMS Developers), building capacity and succession pipelines.
- Ensure implementation of secure development practices and application-level security controls across all systems.

Job Skills and Competencies

- Strong knowledge of enterprise ICT systems and architectures.
- Ability to design and manage microservices architectures, including API-driven and event-driven systems (e.g., Kafka), API gateways and patterns such as Saga and CQRS.
- Proficiency in modern application development technologies, including Java (Spring Framework, Spring Boot, Spring MVC) and .NET (C#, ASP.NET Core), along with ORM tools (Hibernate, JPA, Entity Framework) and frontend frameworks (Angular).
- Expertise in application security, including SSO, token-based authentication, TLS/SSL encryption and secure coding practices aligned with OWASP standards.
- Experience with DevOps practices such as CI/CD pipelines (e.g., Jenkins, Ansible, Azure DevOps), containerization (Docker/Kubernetes) and environment management.
- Strong capability in software quality assurance, including automated testing, performance/load testing, API testing and test environment configuration.
- Familiarity with version control systems (e.g., Git) and collaborative development practices.

Qualifications and Experience

- Bachelor's degree in Computer Science, Information Systems, ICT, or a related field.
- Minimum 5 years' experience in ICT systems development, with proven delivery of enterprise platforms, including tax systems and mobile/web applications.
- At least 2 years in a supervisory or managerial role, leading multi-disciplinary development teams and cross-platform projects.
- Professional certification in Java, C#, .NET, Spring, or an application integration platform (required).
- ICT governance certification is an added advantage.
- Strong understanding of the full software development lifecycle, with emphasis on governance, compliance and quality assurance.
- Experience in IT governance processes, including change management, incident escalation and secure system integrations.
- Proven ability to collaborate effectively within cross-functional teams (developers, testers, DevOps and integration specialists).
- Demonstrated capability to support decision-making within governance frameworks and escalate risks appropriately.
- Must be a self-starter with ability to work under pressure and beyond stipulated hours

- Strong communication and presentation skills along with the ability to work in a highly collaborative environment
- Ability to work with minimum supervision.
- Good organizational, people and time management skills.

SYSTEMS INTEGRATIONS MANAGER – ICT – LEVEL 7 (1 POST)

Key Responsibilities

- Lead the design, development, testing and deployment of secure, scalable integration, mobile and web application systems.
- Oversee system changes, ensuring proper documentation, governance and compliance with change management processes.
- Enforce coding standards, quality assurance practices and continuous improvement across development teams.
- Drive innovation through new system enhancements, proof-of-concept initiatives and emerging technologies.
- Ensure compliance with regulatory, security and data protection standards (e.g., Data Protection Act, ISO/IEC 27001, tax laws).
- Manage risks, internal controls and system integrity, including configuration and version control processes.
- Direct project execution, ensuring timely delivery and alignment with business requirements.
- Lead incident and service request management, including monitoring trends and improving system performance.
- Drive organizational change initiatives and adoption of new technologies and processes.
- Mentor and develop technical teams, fostering knowledge sharing and capability building.
- Promote secure development practices and ensure implementation of application-level security controls

Job Skills and Competencies

- Strong experience in API development and integration (REST, SOAP, JSON, XML) and enterprise integration patterns (e.g., ESB, Kafka, RabbitMQ).
- Proficiency in frontend web development using modern frameworks (Angular, React, Vue).

- Experience in mobile application development (Android, iOS, Flutter, or React Native) with backend/API integration.
- Solid understanding of API design, security (OAuth2, JWT), gateways and versioning.
- Experience integrating with third-party systems (e.g., financial systems, payment gateways, SSO platforms).
- Strong knowledge of application security, secure coding practices, encryption and OWASP standards.
- Familiarity with version control systems (e.g., Git) and collaborative development practices.

Qualifications and Experience

- Bachelor's degree in Computer Science, Information Systems, ICT, or a related field.
- Minimum 5 years' experience in enterprise software application development.
- At least 2 years in a supervisory or managerial role within an ICT environment.
- Professional certification in Java, C#, .NET, Spring, or an application integration platform (required).
- ICT governance certification is an added advantage.
- Must be a self-starter with ability to work under pressure and beyond stipulated hours
- Strong communication and presentation skills along with the ability to work in a highly collaborative environment.
- Ability to work with minimum supervision.

DATABASE ADMINISTRATION MANAGER – ICT – LEVEL 7 (1 POST)

Key Responsibilities

- To lead the governance, resilience and compliance of ZIMRA's Oracle, Windows-based, (primarily SQL Server and related enterprise systems), Postgres and other open-source database platforms
- Ensure strategic alignment, operational integrity and audit readiness of database systems
- Oversee patching schedules, validate backup, performance optimisation, incident classification and systemic problem resolution
- Provide technical and governance authority across database operations,
- Ensure ZIMRA's database estate remains resilient, compliant and aligned with COBIT 2019

- Lead and support enterprise ICT and digital transformation initiatives aligned to ZIMRA strategic objectives and modern tax administration requirements.
- Ensure availability, resilience, optimisation, governance and security of mission-critical and enterprise platforms.
- Implement governance controls, operational standards, audit requirements and compliance frameworks aligned to COBIT 2019, ITIL, ISO/IEC 27001, NIST and ICT policy.
- Mentor graduate trainees, junior analysts and technical teams while promoting knowledge sharing and continuous improvement.

Job Skills and Competencies

- Advanced proficiency in SQL Server administration (SSMS, AlwaysOn Availability Groups, clustering)
- Strong knowledge of query optimisation, indexing strategies and performance tuning
- Experience with enterprise backup and recovery tools (Veeam, Commvault, Bacula, pgBackRest).
- Competence in patch management, configuration baselines and secure deployments for database systems.
- Familiarity with monitoring tools (Nagios, SolarWinds, Prometheus, Zabbix) and proactive alerting.
- Awareness of cloud integration (Azure SQL, AWS RDS) for hybrid database environments
- Strong understanding of enterprise ICT governance, cybersecurity, digital transformation and tax administration environments.
- Knowledge of enterprise governance frameworks including COBIT 2019, ITIL 4, ISO/IEC 27001 and data protection legislation.
- Strong analytical, problem-solving, troubleshooting and operational risk management capability.
- Ability to work effectively in multidisciplinary, high-pressure and mission-critical environments.
- Excellent communication, stakeholder engagement, technical reporting and presentation skills.
- Understanding of enterprise systems integration, operational resilience, audit readiness and compliance management.
- Ability to manage priorities, support operational excellence and drive continuous improvement initiatives.

Qualifications and Experience

- Bachelor's Degree in ICT, Computer Science, Information Systems or equivalent discipline.
- Professional certification in database administration
- At least 5 years' experience supporting large-scale enterprise platforms or public sector digital transformation initiatives.

WINDOWS PLATFORMS MANAGER – ICT - LEVEL 7 (1 POST)

Key Responsibilities

- Design, implement and monitor Windows infrastructure platforms across ZIMRA's ICT environment
- Ensuring system availability, performance and resilience.
- Safeguard critical enterprise systems
- Enforce patching schedules, validate backup routines
- Monitor server health and escalating anomalies.
- Ensures ZIMRA's infrastructure remains resilient, compliant and aligned with COBIT
- Support enterprise ICT and digital transformation initiatives aligned to ZIMRA strategic objectives and modern tax administration requirements.
- Ensure availability, resilience, optimisation, governance and security of mission-critical taxpayer-facing systems and enterprise platforms.
- Implement governance controls, operational standards, audit requirements and compliance frameworks aligned to COBIT, ITIL, ISO/IEC 27001
- Conduct monitoring, incident management, root cause analysis, risk mitigation and continuous service improvement activities.
- Maintain audit-ready documentation, governance artefacts, compliance evidence, technical standards and operational dashboards.
- Collaborate with business units, vendors, financial institutions, regulators and multidisciplinary ICT teams to improve enterprise service delivery.
- Support disaster recovery, business continuity, cyber resilience and operational continuity initiatives across enterprise systems.
- Mentor specialists and technical teams while promoting knowledge sharing and continuous improvement.

Job Skills and Competencies

- Proficiency in enterprise Windows Server administration (Active Directory, Group Policy, DNS, DHCP).
- Strong knowledge of virtualisation platforms (VMware, Hyper-V) and hybrid cloud integration (Azure, AWS).
- Experience with enterprise backup and recovery tools (Veeam, Commvault, Microsoft DPM).
- Competence in patch governance, lifecycle management and configuration baselines.
- Understanding of monitoring tools (Nagios, SolarWinds, SCOM, Zabbix) and performance tuning at enterprise scale.
- Familiarity with cloud integration (Azure, AWS) for hybrid infrastructure
- Understanding of enterprise ICT governance, cybersecurity, digital transformation data protection environments.
- Knowledge of enterprise governance frameworks including COBIT 2019, ITIL 4, ISO/IEC 27001 and data protection legislation.
- Strong analytical, problem-solving, troubleshooting and operational risk management capability.
- Ability to work effectively in multidisciplinary, high-pressure and mission-critical environments.
- Excellent communication, stakeholder engagement, technical reporting and presentation skills.
- Strong understanding of enterprise systems integration, operational resilience, audit readiness and compliance management.
- Ability to manage priorities, support operational excellence and drive continuous improvement initiatives.

Qualifications and Experience

- Bachelor's Degree in ICT, Computer Science, Information Systems or equivalent discipline.
- At least one certification in Microsoft Certified: Windows Server Hybrid Administrator Associate, Azure Administrator Associate, VMware Certified Professional or any equivalent certification
- Relevant enterprise ICT, infrastructure applications development, systems integration, or digital services experience.
- At least 5 years' experience supporting large-scale enterprise platforms or public sector digital transformation initiatives.

ACCESS CONTROL SPECIALIST – ICT – LEVEL 8 (2 POSTS)

Key Responsibilities

- Administer and monitor identity and access controls; enforce authentication standards; validate privileged account usage; escalate anomalies.
- Classify, prioritise and resolve access-related incidents; document access violations; conduct trend analysis to identify recurring issues.
- Maintain access control documentation, evidence trails and compliance artefacts in line with ICT Policy and regulatory standards.
- Identify systemic access risks (e.g., segregation of duties conflicts, excessive privileges); escalate unresolved threats to the Information Assets Security Manager; recommend mitigation measures.
- Maintain inventories of user accounts, roles and entitlements; validate provisioning schedules; ensure secure configurations across systems.
- Apply access control standards; follow escalation protocols; embed continuous improvement practices into access management cycles.
- Manage identity and access lifecycle processes onboarding, role changes, transfers, offboarding and privilege escalations for employees, contractors and third-party accounts.
- Manage privileged accounts and sessions by enforcing session monitoring, just-in-time (JIT) access, multi-factor authentication (MFA), password vaulting and secure credential rotation.
- Coordinate and execute periodic access reviews with application owners and business stakeholders; track remediation of orphaned accounts and excessive permissions.

Job Skills and Competencies

- Proficiency in IAM tools (e.g., CyberArk, Azure AD, Okta, SailPoint).
- Strong knowledge of authentication protocols (LDAP, Kerberos, SAML, OAuth, OpenID Connect).
- Experience with privileged access management and role-based access control (RBAC).
- Competence in maintaining account inventories, entitlement reviews and segregation of duties validation.
- Understanding of directory services, single sign-on (SSO) and multi-factor authentication (MFA).

Qualifications and Experience

- Bachelor's Degree in ICT, Computer Science, Information Systems, Cybersecurity, or equivalent discipline.
- At least 3 years of experience in identity and access management, authentication systems, or cybersecurity operations.
- At least one professional certification in cybersecurity or Identity and Access Administration or related certification
- Exposure to access provisioning tools, privileged account management and incident escalation.

APPLICATION SECURITY SPECIALIST – ICT – LEVEL 8 (3 POSTS)

Key Responsibilities

- Implement and monitor application security controls, including secure coding standards, vulnerability scanning and patch validation
- Classify, prioritise and resolve application security alerts; document known errors and conduct trend analysis
- Maintain application security documentation, evidence trails and compliance artefacts in line with ICT Policy and regulatory standards
- Identify application vulnerabilities, escalate unresolved threats and recommend mitigation measures to the Security Architecture Manager
- Maintain inventories of enterprise applications, validate patch levels and ensure secure configurations
- Document lessons learned from application incidents, update secure coding guidelines and contribute to the governance knowledge base
- Apply application security standards, conduct peer reviews and embed continuous improvement practices; maintain peer review compliance
- Mentor developers, graduate trainees and interns in secure coding practices; contribute to skills development and maintain skills matrix updated quarterly
- Escalate systemic threats, recommend mitigation measures, maintain risk register updates and track mitigation actions
- Participate in cybersecurity drills, red team/blue team exercises and disaster recovery simulations;
- Any other duties as may be assigned by the Security Architecture Manager.

Job Skills and Competencies

- Proficiency in application security testing tools (e.g., OWASP ZAP, Burp Suite, Veracode).

- Demonstrate knowledge of secure coding practices across languages (Java, .NET, PHP, Python).
- Experience working in multi-disciplinary teams (IT, Risk, Audit, Compliance) to ensure coordinated response.
- Self-starter with ability to work under pressure, including in 24/7 monitoring environments
- Strong communication and presentation skills along with the ability to work in a highly collaborative environment
- Ability to plan and exceptional time management skills
- Ability to work with minimum supervision.
- Good organizational and people management skills.

Qualifications and Experience

- A graduate Degree in Computer Science or Information & Communication Technology or equivalent qualification.
- Must have at least one of the following Certification: CISA; CISM; CISSP; Certified Secure Software Lifecycle Professional (CSSLP); OWASP Application Security Verification Standard (ASVS) Practitioner; or a comparable security certification.
- Minimum of three (3) year experience in ICT of which One (1) year should be in ICT security, application development, application security or Software Development Assurance areas

DATA LOSS PREVENTION SPECIALIST – ICT – LEVEL 8 (2 POSTS)

Key Responsibilities

- Design, implement and maintain the organisation's DLP program and roadmap.
- Deploy and configure DLP tools across endpoints, network, email, cloud apps (CASB integration) and data repositories .
- Create, tune and manage detection rules, content classifiers, fingerprints, regex patterns and policy templates to identify sensitive data (PII, PHI, financial, IP, credentials).
- Maintain and improve data discovery and classification workflows; integrate with data classification tools and the organization's data catalog.
- Monitor DLP alerts, triage incidents, validate true positives vs false positives and determine severity and impact.

- Lead or support containment and remediation actions (blocking, quarantine, encryption, revocation of access), coordinating with IT and incident response teams.
- Maintain incident logs, evidence and timelines for investigations and for audit/regulatory purposes,Conduct data flow mapping and risk assessments to identify where sensitive data resides and how it moves (in use, in motion, at rest).
- Evaluate and reduce insider risk through monitoring, behavioural analytics and integration with UEBA or insider-risk tools.
- Develop and maintain DLP policies, playbooks, escalation paths and standard operating procedures.
- Ensure compliance with relevant laws and standards (ISO27001, Data Protection Act, NIST, COBIT 2019) and provide evidence for audits.

Job Skills and Competencies

- Hands-on experience with DLP platforms (e.g., Microsoft Purview, Netskope).
- Familiarity with data discovery, classification, regular expressions, fingerprinting and content inspection techniques.
- Strong understanding of networking, email systems (Exchange, SMTP), cloud storage (AWS, Azure, GCP), endpoints and encryption technologies.
- Experience integrating DLP with SIEM, CASB, IAM and endpoint agents.
- Scripting/automation skills (Python, PowerShell) and comfort reading logs and telemetry
- Knowledge of Zimbabwe's Data Protection and Cyber Security Act, plus relevant international standards (ISO/IEC 27001, GDPR, PCI-DSS, NIST CSF).

Qualifications and Experience

- Bachelor's Degree in ICT, Computer Science, Information Systems, Cybersecurity, or equivalent discipline.
- Minimum of three (3) year experience in ICT of which One (1) year should be in ICT security, data loss prevention, data classification and policy formulation.
- Professional certification in cybersecurity (minimum one recognised certification) such as Certified Information Systems Security Professional (CISSP), Certified Data Privacy Solutions Engineer (CDPSE)
- Vendor-specific certifications (Forcepoint Data Loss Prevention (DLP) System Engineer, Proofpoint Certified DLP Specialist (covering endpoint, CASB and email) are an added advantage

DATABASE SECURITY SPECIALIST – ICT – LEVEL 8 (2 POSTS)

Key Responsibilities

- Implement and monitor database security controls, including encryption standards, access control policies and database activity monitoring.
- Classify, prioritise and resolve database security alerts; document known errors and conduct trend analysis.
- Maintain database security documentation, evidence trails and compliance artefacts in line with ICT Policy and regulatory standards.
- Identify database vulnerabilities, escalate unresolved threats and recommend mitigation measures to the Security Architecture Manager.
- Maintain inventories of enterprise databases, validate patch levels, encryption baselines and ensure secure configurations.
- Document lessons learned from database incidents, update database security procedures and playbooks and contribute to the governance knowledge base.
- Monitor and protect ZIMRA's critical enterprise data repositories; contribute to intelligence-enriched monitoring by correlating threat feeds and indicators of compromise (IOCs) against real-time database alerts.
- Participate in cybersecurity drills, red team/blue team exercises and disaster recovery simulations
- Any other duties as may be assigned by the Security Architecture Manager.

Job Skills and Competencies

- Experience working in multi-disciplinary teams (IT, Risk, Audit, Compliance) to ensure coordinated governance and response.
- Proficiency in database platforms (Oracle, Microsoft SQL Server, MySQL, PostgreSQL); strong knowledge of database encryption, access control and activity monitoring.
- Understanding of common security standards: PCI DSS, ISO 27001, COBIT, NIST; familiarity with ITIL service management.
- Strong communication and presentation skills; self-starter with ability to work under pressure including in 24/7 monitoring environments.
- Good organizational, people and time management skills.

Qualifications and Experience

- Bachelor's Degree in ICT, Computer Science, Information Systems, Cybersecurity, or equivalent discipline.
- Must have at least one of the following certifications: Oracle Certified Professional (OCP) - Database Security; Microsoft SQL Server Security Certification; GIAC Certified Database Security Administrator (GCDSA); or a comparable security certification.
- Minimum of three (3) year experience in ICT of which One (1) year should be in database administration, database security or information assurance
- Exposure to database hardening, encryption, access control, vulnerability scanning, patch validation and remediation actions.

INCIDENT RESPONSE SPECIALIST – ICT – LEVEL 8 (1 POST)

Key Responsibilities

- Lead the containment, eradication and recovery phases of escalated cybersecurity incidents, ensuring incident closure SLA compliance and recovery time objectives are met
- Execute incident response playbooks and coordinate forensic evidence collection, maintaining playbook adherence and complete evidence trails
- Ensure incident documentation meets regulatory and audit standards, maintaining compliance scores and producing audit-defensible artefacts).
- Escalate systemic threats, recommend mitigation measures, maintain risk register updates and track mitigation actions
- Document lessons learned, update SOC playbooks and contribute to post-incident reviews ensuring playbooks are updated per incident cycle
- Apply SOC standards, conduct peer reviews of incident documentation and embed continuous improvement practices; maintain peer review compliance
- Provide technical guidance and mentoring to SOC Analysts during incident response, contributing to skills development and maintaining skills matrix updated quarterly
- Coordinate forensic evidence collection, eradication procedures and service restoration in line with SOC playbooks across critical systems
- Participate in cybersecurity drills, red team/blue team exercises and disaster recovery simulations.
- Contribute to intelligence-enriched monitoring by correlating threat feeds and indicators of compromise (IOCs) against real-time alerts in the SIEM platform.

Job Skills and Competencies

- Understanding of common security standards and regulations relating to information systems (e.g., PCI DSS, ISO27001, COBIT, NIST)
- Demonstrate exposure to incident detection and escalation, service request handling, vulnerability identification and containment actions
- Experience working in multi-disciplinary teams (IT, Risk, Audit, Compliance) to ensure coordinated response.
- Strong knowledge of network protocols, log analysis and intrusion detection systems (IDS/IPS).
- Experience with endpoint detection and response (EDR) tools; familiarity with threat intelligence feeds, correlation rules and basic forensic analysis.
- A strong understanding of common security standards and regulations relating to information systems as well as risk related control frameworks and practices such as ITIL, ISO, COBIT, NIST Cyber Security

Qualifications and Experience

- Bachelor's Degree in ICT, Computer Science, Information Systems, Cybersecurity, or equivalent discipline.
- Must have at least one of the following Certification: CISM; CISSP; CEH; CHFI; CompTIA Security+; GIAC Security Essentials (GSEC); SANS Cyber Incident Response (CIR GIAC Cyber Threat Intelligence (GCTI) COBIT; ISO 27001, ITIL or a comparable security certification.
- Minimum of three (3) year experience in ICT of which One (1) year should be in ICT security, or equivalent experience in areas such as ICT Risk Management or ICT Audit.

NETWORK SECURITY SPECIALIST – ICT – LEVEL 8 (1 POST)

Key Responsibilities

- Design, configure and deploy firewalls, IDS/IPS, VPNs and segmentation policies to detect anomalies and escalate network incidents
- Classify, prioritise and resolve network security alerts; document known errors and conduct trend analysis
- Maintain network security documentation, evidence trails and compliance artefacts in line with ICT Policy and regulatory standards
- Identify vulnerabilities in network infrastructure, escalate unresolved threats and recommend mitigation measures to the Security Architecture Manager
- Maintain inventories of routers, switches, firewalls and network appliances; validate firmware versions and secure configurations

- Document lessons learned from network incidents, update network security procedures and playbooks and contribute to the governance knowledge base
- Apply network security standards, conduct peer reviews of configuration documentation and embed continuous improvement practices; maintain peer review compliance
- Implement advanced monitoring controls, validate deficiency reports and recommend corrective actions; submit weekly deficiency reports to the Security Architecture Manager
- Monitor and protect ZIMRA's critical enterprise network infrastructure; contribute to intelligence-enriched monitoring by correlating threat feeds and indicators of compromise (IOCs) against real-time network alerts.
- Participate in cybersecurity drills, red team/blue team exercises and disaster recovery simulations
- Any other duties as may be assigned by the Security Architecture Manager.

Job Skills and Competencies

- Understanding of common security standards and regulations relating to information systems (e.g., PCI DSS, ISO27001, COBIT, NIST)
- Strong knowledge of network protocols, log analysis, intrusion detection/prevention systems (IDS/IPS) and packet analysis.
- Proficiency in firewall platforms; experience with VPNs, segmentation policies and secure routing.
- Self-starter with ability to work under pressure, including in 24/7 monitoring environments
- Strong communication and presentation skills along with the ability to work in a highly collaborative environment
- Ability to plan and exceptional time management skills
- Ability to work with minimum supervision.
- Good organizational and people management skills.
- A team player who is innovative and analytical.

Qualifications and Experience

- Bachelor’s Degree in ICT, Computer Science, Information Systems, Cybersecurity, or equivalent discipline.

- Must have at least one of the following Certification: CISA; CISM; CISSP; CompTIA Security+; GIAC Security Essentials (GSEC); Cisco Certified Network Associate (CCNA Security); or a comparable security certification.
- Minimum of three (3) year experience in ICT of which One (1) year should be in ICT security, or equivalent experience in areas such as Network Administration, Network Security or Infrastructure Security.
- Exposure to firewall management, IDS/IPS configuration, VPN management, vulnerability identification and containment actions.

SECURITY OPERATIONS SPECIALIST – ICT – LEVEL 8 (4 POSTS)

Key Responsibilities

- Investigate escalated Tier 2/Tier 3 cybersecurity incidents, refine SIEM detection rules and coordinate forensic evidence collection, ensuring incident closure SLA compliance and evidence trail completeness
- Classify escalated incidents, prioritise containment actions and determine whether to escalate further to the SOC Manager or enterprise response teams; manage known errors and conduct trend analysis
- Ensure incident investigation documentation meets regulatory and audit standards; produce forensic reports and compliance artefacts, maintaining compliance scores
- Identify systemic threats, recommend mitigation measures and escalate to the SOC Manager or maintain risk register updates and track mitigation actions
- Document lessons learned, update SOC detection playbooks with new correlation rules and contribute to post-incident reviews; ensure playbooks are updated per incident cycle
- Apply SOC engineering standards, conduct peer reviews of Analyst incident documentation and embed continuous improvement practices; maintain peer review compliance
- Implement advanced monitoring controls, validate deficiency reports from SOC Analysts and recommend corrective actions; submit weekly deficiency reports to the SOC Manager
- Participate in cybersecurity drills, red team/blue team exercises and disaster recovery simulations
- Contribute to intelligence-enriched monitoring by correlating threat feeds and indicators of compromise (IOCs) against real-time alerts in the SIEM platform.

Job Skills and Competencies

- Understanding of common security standards and regulations relating to information systems (e.g., PCI DSS, ISO27001, COBIT, NIST)
- Demonstrate exposure to incident detection and escalation, service request handling, vulnerability identification and containment actions
- Experience working in multi-disciplinary teams (IT, Risk, Audit, Compliance) to ensure coordinated response.
- Strong knowledge of network protocols, log analysis and intrusion detection systems (IDS/IPS).
- Experience with endpoint detection and response (EDR) tools; familiarity with threat intelligence feeds, correlation rules and basic forensic analysis.
- A strong understanding of common security standards and regulations relating to information systems as well as risk related control frameworks and practices such as ITIL, ISO, COBIT, NIST Cyber Security

Qualifications and Experience

- Bachelor's Degree in ICT, Computer Science, Information Systems, Cybersecurity, or equivalent discipline.
- Must have at least one of the following Certification: CISA; CISM; CISSP; CEH; CompTIA Security+; GIAC Security Essentials (GSEC); COBIT; ISO 27001, ITIL or a comparable security certification.
- Minimum of three (3) year experience in ICT of which One (1) year should be in ICT security, or equivalent experience in areas such as ICT Risk Management or ICT Audit.

THREAT INTELLIGENCE SPECIALIST – ICT – LEVEL 8 (2 POSTS)

Key Responsibilities

- Collect, validate and analyse cyber threat intelligence from internal telemetry, external feeds, Open Source Intelligent (OSINT) and information sharing communities; profile adversary TTPs and disseminate actionable intelligence to the SOC team
- Classify intelligence-driven alerts, prioritise threat escalations and enrich Tier 2/Tier 3 incident investigations with contextual intelligence; coordinate with SOC Engineers on response actions
- Produce intelligence reports, evidence trails and compliance artefacts that meet regulatory and audit standards; maintain documentation accuracy and ensure forensic readiness

- Identify emerging threats, geopolitical risk indicators and systemic vulnerabilities; escalate actionable risks to the SOC Manager and enterprise risk committees with recommended mitigation measures
- Document threat intelligence findings, update SOC detection playbooks with new IOCs and TTPs and contribute to post-incident reviews and lessons learned processes
- Integrate intelligence outputs into monitoring controls; identify gaps in threat detection coverage and recommend corrective actions to the SOC Manager
- Monitor threat landscape for risks targeting ZIMRA's critical enterprise System.
- Participate in red team/blue team exercises, cybersecurity drills and disaster recovery simulations
- Contribute to intelligence-enriched monitoring by correlating threat feeds and indicators of compromise (IOCs) against real-time alerts in the SIEM platform.
- Any other duties as may be assigned by the Security Operations Manager.

Job Skills and Competencies

- Demonstrate exposure to intelligence collection, adversary profiling, malware campaign analysis and dissemination of actionable intelligence.
- Experience working in multi-disciplinary teams (IT, Risk, Audit, Compliance, Legal, CERTs) to ensure coordinated intelligence sharing and incident response.
- Proficiency in threat intelligence platforms (TIPs) and SIEM integration, strong knowledge of network protocols, log correlation and adversary TTP analysis.
- Experience with endpoint detection and response (EDR) tools, malware sandboxing, open-source intelligence (OSINT) and source validation techniques.
- Familiarity with threat intelligence frameworks including MITRE ATT&CK, Diamond Model and Kill Chain; competence in malware analysis and IOC management.
- Experience with endpoint detection and response (EDR) tools; familiarity with threat intelligence feeds, correlation rules and basic forensic analysis.
- Self-starter with ability to work under pressure, including in 24/7 monitoring environments

Qualifications and Experience

- Bachelor’s Degree in ICT, Computer Science, Information Systems, Cybersecurity, or equivalent discipline.

- Must have at least one of the following Certification: CISA; CISM; CISSP; CEH; CHFI; CompTIA Security+; GIAC Security Essentials (GSEC); Certified Threat Intelligence Analyst (CTIA); GIAC Cyber Threat Intelligence (GCTI) COBIT; ISO 27001, ITIL or a comparable security certification.
- Minimum of three (3) year experience in ICT of which One (1) year should be in ICT security, or equivalent experience in areas such as ICT Risk Management or ICT Audit.
- Understanding of common security standards and regulations relating to information systems (e.g., PCI DSS, ISO27001, COBIT, NIST)

VULNERABILITY MANAGEMENT SPECIALIST – ICT – LEVEL 8 (2 POSTS)

Key Responsibilities

- Conduct vulnerability scans across ICT assets; validate patch levels; monitor remediation effectiveness; escalate unresolved vulnerabilities.
- Classify, prioritise and resolve vulnerability alerts; document known weaknesses; conduct trend analysis to identify recurring issues.
- Maintain vulnerability management documentation, evidence trails and compliance artefacts in line with ICT Policy and regulatory standards.
- Identify systemic vulnerabilities; escalate unresolved threats to the Identity and Access Manager; recommend mitigation measures for enterprise risk registers.
- Document lessons learned from vulnerability remediation; update procedures; contribute to governance knowledge base.
- Maintain inventories of ICT assets; validate firmware versions and patch schedules
- Document lessons learned from vulnerability remediation; update procedures; contribute to governance knowledge base.
- Apply vulnerability management standards; follow escalation protocols; embed continuous improvement practices into remediation cycles.
- Contribute to security awareness and training for remediation owners to improve patching and secure-config processes.
- Any other duties as may be assigned by the Information Security Assets Manager.

Job Skills and Competencies

- Exposure to vulnerability scanning tools, patch validation, remediation actions and risk escalation.
- Experience working in multi-disciplinary teams (IT, Risk, Audit, Compliance) to ensure coordinated governance and response.

- Enables effective specialist-level decision-making without reference to a superior, within approved vulnerability management standards and escalation thresholds
- Proficiency in vulnerability scanning tools (e.g., Nessus, Qualys, Rapid7 InsightVM).
- Strong knowledge of patch management and remediation processes.
- Familiarity with secure configuration baselines across operating systems, databases and applications.
- Competence in maintaining ICT asset inventories and validating patch schedules.
- Understanding of penetration testing methodologies and exploit validation.

Qualifications and Experience

- Bachelor's Degree in ICT, Computer Science, Information Systems, Cybersecurity, or equivalent discipline.
- Professional certification in vulnerability management or cybersecurity (minimum one recognised certification) ; GIAC Vulnerability Assessment (GVA) ,Offensive Security Certified Professional (OSCP) ,ISO/IEC 27001 Lead Implementer or Auditor, Vendor-specific certifications (Nessus, Qualys, Rapid7 InsightVM) or similar certifications.
- At least 3 years of experience in vulnerability management, penetration testing, or cybersecurity operations.

APPLICATIONS DEVELOPER, FDMS - ICT – LEVEL 8 (3 POSTS)

Key Responsibilities

- Enhance and optimize existing systems, ensuring scalability, performance and reliability.
- Architect and implement robust integration solutions across internal and external systems, ensuring high availability and interoperability.
- Oversee and support resolution of complex technical issues ensuring timely incident resolution.
- Translate complex business and taxpayer requirements into secure, scalable and user-centric mobile and web solutions.
- Adhere to software development standards, coding guidelines and best practices.
- Implement secure coding practices, including proactive vulnerability mitigation (OWASP Top 10), secure authentication/authorization, encryption and data protection strategies.
- Develop technical documentation, including architecture designs, integration specifications and post-implementation reviews.

- Apply IT governance frameworks (e.g., COBIT, ITIL) and ensure compliance with organizational and regulatory standards.
- Implement knowledge sharing, code quality and continuous improvement within the development team.
- Collaborate with cross-functional teams (developers, testers, UX designers, DevOps and integration specialists) to deliver high-quality solutions.
- Communicate effectively with both technical and non-technical stakeholders, including senior leadership and contribute to strategic decision-making.

Job Skills and Competencies

- Advanced proficiency in Java (Spring Boot, Hibernate, Java EE) and C#/.NET for enterprise-grade application development.
- Strong expertise in RESTful APIs, GraphQL, microservices architecture and secure system integrations.
- Experience with both relational and NoSQL databases (e.g., MySQL, PostgreSQL, MongoDB).
- Familiarity with CI/CD pipelines and tools (e.g., Jenkins, GitLab, GitHub Actions), as well as containerization technologies (Docker, Kubernetes).
- Experience with testing and monitoring tools (e.g., Postman, SoapUI, JMeter) to ensure system accuracy, performance and reliability.
- Possess strong Business Ethics
- Clean Class 4 drivers license

Qualifications and Experience

- Bachelor's degree in Computer Science, Information Systems, Business Studies & Computer Science, or a related field.
- Minimum 2 years' experience in application development, with strong proficiency in C#/.NET and Java.
- Professional certification in systems development (any programming language) is required.

APPLICATIONS DEVELOPER, INTEGRATIONS – ICT – LEVEL 8 (4 POSTS)

Key Responsibilities

- Design, develop and support enterprise integration solutions and backend integration services.
- Develop and manage APIs to enable seamless integration across mobile, web and enterprise systems.
- Build and maintain integration interfaces using technologies such as BizTalk, Azure Service Bus, WSO2, MuleSoft, Apache Camel, MQ Series and other ESB platforms.
- Contribute to system security, performance optimization and continuous improvement of web and mobile platforms (including UX and search optimization).
- Define technical architecture and design for integration solutions and collaborate with development teams on new and existing applications.
- Modify and enhance applications to meet evolving business requirements and resolve system issues.
- Ensure adherence to established software development standards, policies and best practices.
- Monitor, maintain and support deployed systems to ensure reliability and performance.
- Perform any other duties as assigned.

Job Skills and Competencies

- Hands-on experience with integration technologies such as Microsoft BizTalk, Azure Service Bus, WSO2, MuleSoft, Apache Camel, MQ Series and ESB platforms.
- Experience with technologies including .NET/C#, Spring Framework, Hibernate, Web Services, IIS, HTML and XML-related tools (XSD, XSLT, XPath, XQuery) is an added advantage.
- Strong understanding of web technologies and protocols, including HTTP/S, REST, SOAP, JSON, FTP, SSH and SMTP.
- Possess strong Business Ethics
- Clean Class 4 drivers license

Qualifications and Experience

- Bachelor's degree in Computer Science, Information Systems, Business Studies & Computer Science, or a related field.
- Proven experience in application development, with at least 2 years in systems integration using C#/.NET and Java.
- Professional certification in systems development (in any programming language) is required.

WINDOWS SYSTEMS DOMAIN CONTROLLER SPECIALIST - ICT – LEVEL 8 (1 POST)

Key Responsibilities

- Design, implement and monitor Windows domain controllers infrastructure across ZIMRA's ICT environment
- Ensure system availability, performance and resilience
- Safeguard critical enterprise systems by enforcing patching schedules, validating backup routines, monitoring server health and escalating anomalies
- Ensure ZIMRA's domain controllers infrastructure remains resilient, compliant and aligned with COBIT 2019
- Implement governance controls, operational standards, audit requirements and compliance frameworks aligned to COBIT, ITIL, ISO/IEC 27001, NIST and ICT policy.
- Conduct monitoring, incident management, root cause analysis, risk mitigation and continuous service improvement activities.
- Maintain audit-ready documentation, governance artefacts, compliance evidence, technical standards and operational dashboards.
- Collaborate with business units, vendors, financial institutions, regulators and multidisciplinary ICT teams to improve enterprise service delivery.
- Support disaster recovery, business continuity, cyber resilience and operational continuity initiatives across enterprise systems.
- Mentor graduate trainees, junior analysts and technical teams while promoting knowledge sharing and continuous improvement.

Job Skills and Competencies

- Proficiency in Windows Server administration (Domain Controllers, Active Directory, Group Policy, DNS, DHCP, Tiering).
- Strong knowledge of virtualisation platforms (VMware, Hyper-V).
- Experience with backup and recovery tools (Veeam, Commvault, Microsoft DPM).
- Competence in patch management and configuration baselines.
- Understanding of monitoring tools (Nagios, SolarWinds, SCOM) and performance tuning.
- Familiarity with cloud integration (Azure, AWS) for hybrid infrastructure
- Understanding of enterprise ICT governance, cybersecurity, digital transformation and tax administration environments.

- Knowledge of enterprise governance frameworks including COBIT 2019, ITIL 4, ISO/IEC 27001 and data protection legislation.
- Strong analytical, problem-solving, troubleshooting and operational risk management capability.
- Ability to work effectively in multidisciplinary, high-pressure and mission-critical environments.
- Excellent communication, stakeholder engagement, technical reporting and presentation skills.
- Strong understanding of enterprise systems integration, operational resilience, audit readiness and compliance management.
- Ability to manage priorities, support operational excellence and drive continuous improvement initiatives.

Qualifications and Experience

- Bachelor's Degree in ICT, Computer Science, Information Systems or equivalent discipline.
- Certification in Microsoft Identity and Access Administrator, Windows Server Hybrid Administrator Associate or equivalent is mandatory
- Relevant enterprise in ICT, infrastructure, cybersecurity, or digital services experience.
- At least 3 years' experience supporting large-scale enterprise platforms or public sector digital transformation initiatives.

WINDOWS SYSTEMS EXCHANGE SPECIALIST – ICT – LEVEL 8 (1 POST)

Key Responsibilities

- Design, implement and monitor Windows infrastructure platforms across ZIMRA's Exchange ICT environment
- Ensure system availability, performance and resilience
- Safeguard critical enterprise systems by enforcing patching schedules, validating backup routines, monitoring server health and escalating anomalies
- Ensure ZIMRA's infrastructure remains resilient, compliant and aligned with COBIT 2019
- Support enterprise ICT and digital transformation initiatives aligned to ZIMRA strategic objectives and modern tax administration requirements.
- Ensure availability, resilience, optimisation, governance and security of mission-critical taxpayer-facing systems and enterprise platforms.

- Implement governance controls, operational standards, audit requirements and compliance frameworks aligned to COBIT, ITIL, ISO/IEC 27001, NIST and ICT policy.
- Conduct monitoring, incident management, root cause analysis, risk mitigation and continuous service improvement activities.
- Maintain audit-ready documentation, governance artefacts, compliance evidence, technical standards and operational dashboards.
- Collaborate with business units, vendors, financial institutions, regulators and multidisciplinary ICT teams to improve enterprise service delivery.
- Support disaster recovery, business continuity, cyber resilience and operational continuity initiatives across enterprise systems.
- Mentor graduate trainees, junior analysts and technical teams while promoting knowledge sharing and continuous improvement.

Job Skills and Competencies

- Proficiency in Windows Server administration (Exchange, Active Directory, Group Policy, DNS, DHCP).
- Strong knowledge of virtualisation platforms (VMware, Hyper-V).
- Experience with backup and recovery tools (Veeam, Commvault, Microsoft DPM).
- Competence in patch management and configuration baselines.
- Understanding of monitoring tools (Nagios, SolarWinds, SCOM) and performance tuning.
- Familiarity with cloud integration (Azure, AWS) for hybrid infrastructure
- Understanding of enterprise ICT governance, cybersecurity, digital transformation and tax administration environments.
- Knowledge of enterprise governance frameworks including COBIT 2019, ITIL 4, ISO/IEC 27001, NIST CSF, GDPR and data protection legislation.
- Strong analytical, problem-solving, troubleshooting and operational risk management capability.
- Ability to work effectively in multidisciplinary, high-pressure and mission-critical environments.
- Excellent communication, stakeholder engagement, technical reporting and presentation skills.
- Strong understanding of enterprise systems integration, operational resilience, audit readiness and compliance management.

- Ability to manage priorities, support operational excellence and drive continuous improvement initiatives.

Qualifications and Experience

- Bachelor's Degree in ICT, Computer Science, Information Systems or equivalent discipline.
- Certification in Microsoft 365 Messaging Administrator Associate, Windows Server Hybrid Administrator Associate or equivalent is mandatory.
- Relevant enterprise ICT, infrastructure, cybersecurity, or digital services experience.
- At least 3 years' experience supporting large-scale enterprise platforms, taxpayer-facing systems, or public sector digital transformation initiatives.

DATABASE ADMINISTRATOR – ICT – LEVEL 8 (1 POST)

Key Responsibilities

- Administer, monitor and safeguard ZIMRA's Postgres and other Open Source Databases
- Ensure resilience, performance and compliance
- Enforce patching schedules, validates and restores backups, monitors database health, optimises queries and escalates systemic anomalies
- Provide technical authority in database operations
- Mentor Junior Database Administrators and ensures ZIMRA's databases remain resilient, compliant and aligned with COBIT 2019
- Conduct monitoring, incident management, root cause analysis, risk mitigation and continuous service improvement activities.
- Maintain audit-ready documentation, governance artefacts, compliance evidence, technical standards and operational dashboards.
- Collaborate with business units, vendors, financial institutions, regulators and multidisciplinary ICT teams to improve enterprise service delivery.
- Support disaster recovery, business continuity, cyber resilience and operational continuity initiatives across enterprise systems.
- Mentor graduate trainees, junior analysts and technical teams while promoting knowledge sharing and continuous improvement.

Job Skills and Competencies

- Advanced proficiency in ProstgreSQL administration (pgAdmin, AlwaysOn Availability Groups, clustering).

- Familiarity with Linux/UNIX or Windows operating system.
- Strong SQL knowledge for querying, scripting and performance tuning.
- Experience with backup and recovery tools (Veeam).
- Competence in patch management, configuration baselines and secure deployments for database systems.
- Familiarity with monitoring tools (SolarWinds, Zabbix) and proactive alerting.
- Awareness of cloud integration (AWS RDS) for hybrid database environments
- Knowledge of enterprise governance frameworks including COBIT 2019, ITIL 4, ISO/IEC 27001 and data protection legislation.
- Strong analytical, problem-solving, troubleshooting and operational risk management capability.
- Ability to work effectively in multidisciplinary, high-pressure and mission-critical environments.
- Excellent communication, stakeholder engagement, technical reporting and presentation skills.
- Strong understanding of enterprise systems integration, operational resilience, audit readiness and compliance management.
- Ability to manage priorities, support operational excellence and drive continuous improvement initiatives.

Qualifications and Experience

- Bachelor's Degree in ICT, Computer Science, Information Systems, or equivalent discipline.
- Certification in PostgreSQL or equivalent
- Relevant enterprise ICT, infrastructure, cybersecurity or digital services experience.
- At least 3 years' experience supporting large-scale enterprise platforms, taxpayer-facing systems, or public sector digital transformation initiatives.

OPEN SYSTEMS SPECIALIST – ICT – LEVEL 8 (1 POST)

Key Responsibilities

- Design, implement and monitor open systems infrastructure platforms (Linux, UNIX and hybrid environments) across ZIMRA's ICT environment
- Ensure system availability, performance and resilience.

- Safeguards critical enterprise systems by enforcing patching schedules, validating backup routines, monitoring server health and escalating anomalies.
- Ensures ZIMRA's infrastructure remains resilient, compliant and aligned with COBIT
- Support enterprise ICT and digital transformation initiatives aligned to ZIMRA strategic objectives and modern tax administration requirements.
- Ensure availability, resilience, optimisation, governance and security of mission-critical systems and enterprise platforms.
- Implement governance controls, operational standards, audit requirements and compliance frameworks aligned to COBIT, ITIL, ISO/IEC 27001, NIST and ICT policy.
- Conduct monitoring, incident management, root cause analysis, risk mitigation and continuous service improvement activities.
- Maintain audit-ready documentation, governance artefacts, compliance evidence, technical standards and operational dashboards.
- Collaborate with business units, vendors, financial institutions, regulators and multidisciplinary ICT teams to improve enterprise service delivery.
- Support disaster recovery, business continuity, cyber resilience and operational continuity initiatives across enterprise systems.
- Mentor graduate trainees, junior analysts and technical teams while promoting knowledge sharing and continuous improvement.

Job Skills and Competencies

- Proficiency in Linux/Open Systems administration (user/group management, shell scripting, systemd, cron, SELinux, DNS, DHCP equivalents).
- Strong knowledge of virtualisation platforms (VMware, KVM (Kernel-based Virtual Machine) or OpenStack).
- Experience with backup and recovery tools (Veeam, Commvault, rsync, tar, Bacula, or other Linux-based backup tools).
- Competence in patch management and configuration baselines.
- Understanding of monitoring tools (Nagios, SolarWinds, Prometheus, Zabbix, or equivalent Linux monitoring tools) and performance tuning.
- Understanding of enterprise ICT governance, cybersecurity, digital transformation and tax administration environments.
- Knowledge of enterprise governance frameworks including COBIT 2019, ITIL 4, ISO/IEC 27001 and data protection legislation.

- Strong analytical, problem-solving, troubleshooting and operational risk management capability.
- Ability to work effectively in multidisciplinary, high-pressure and mission-critical environments.
- Excellent communication, stakeholder engagement, technical reporting and presentation skills.
- Strong understanding of enterprise systems integration, operational resilience, audit readiness and compliance management.
- Ability to manage priorities, support operational excellence and drive continuous improvement initiatives.

Qualifications and Experience

- Bachelor's Degree in ICT, Computer Science, Information Systems, Cybersecurity, or equivalent discipline.
- Certification in Linux such as Red Hat Certified System Administrator (RHCSA), Red Hat Certified Engineer (RHCE) or equivalent
- Relevant enterprise ICT, infrastructure, cybersecurity, or digital services experience.
- At least 3 years' experience supporting large-scale enterprise platforms, taxpayer-facing systems, or public sector digital transformation initiatives.

JUNIOR SECURITY OPERATIONS CENTRE SPECIALIST – ICT – LEVEL 9 (5 POSTS)

Key Responsibilities

- Monitor SIEM platforms, IDS/IPS alerts and security dashboards in real time; detect anomalies and cybersecurity events and escalate confirmed incidents to SOC Engineers.
- Classify, prioritise and handle Tier 1 security alerts and service requests; document known errors, conduct trend analysis and escalate unresolved incidents within defined SLAs
- Produce accurate incident detection records, escalation logs and compliance artefacts in line with ICT Policy and regulatory standards
- Identify potential vulnerabilities and network anomalies during monitoring activities; document and escalate unresolved threats to SOC Specialists for further investigation
- Document lessons learned from detected incidents and contribute to updates of SOC detection playbooks and escalation procedures
- Apply SOC monitoring standards, participate in peer reviews of incident documentation and contribute to continuous improvement of detection and escalation processes

- Implement Tier 1 monitoring controls, identify and report deficiencies in monitoring coverage and recommend corrective actions to the SOC Specialists
- Contribute to intelligence-enriched monitoring by correlating threat feeds and indicators of compromise (IOCs) against real-time alerts in the SIEM platform.
- Any other duties as may be assigned by the Security Operations Specialist & Security Operations Manager.

Job Skills and Competencies

- Experience with endpoint detection and response (EDR) tools; familiarity with threat intelligence feeds, correlation rules and basic forensic analysis.
- A strong understanding of common security standards and regulations relating to information systems as well as risk related control frameworks and practices such as ITIL, ISO, COBIT, NIST Cyber Security
- Self-starter with ability to work under pressure and beyond stipulated hours
- Strong communication and presentation skills along with the ability to work in a highly collaborative environment

Qualifications and Experience

- Bachelor's Degree in ICT, Computer Science, Information Systems, Cybersecurity, or equivalent discipline.
- Must have at least one of the following Certification: CEH; CompTIA Security+; Certified SOC Analyst (CSA); GIAC Security Essentials (GSEC); COBIT; ISO 27001, ITIL or a comparable ICT/Security certification.
- Minimum of two (2) years' experience in ICT security, SOC operations, or equivalent experience in ICT Operations/Cybersecurity roles
- Demonstrate exposure to incident detection and escalation, service request handling, vulnerability identification and containment actions.

Interested candidates should submit applications, accompanied by a detailed Curriculum Vitae by **19 May 2026. All applications should be emailed to ZimraRecruitment@zimra.co.zw with the position title clearly stated in the email subject line, e.g. Head ICT Operations & Service Delivery – ICT Level 5.** The applications should be addressed to:

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.