

OPERATIONS

Senior Manager - ICT

DEPARTMENT	REPORTS TO	LEVEL	EXPERIENCE	LOCATION
Operations	Chief Operations Officer	Leadership	8+ years	Nairobi, Kenya

Role Purpose

The Senior Manager - ICT is responsible for providing strategic and operational leadership in the development, implementation and management of ACS's information and communication technology infrastructure, systems and digital solutions.

The role ensures the availability, security, reliability and scalability of technology platforms supporting healthcare claims administration, pre-authorisation, member and provider services, data management and business operations.

The Senior Manager - ICT will drive digital transformation, strengthen information security and data protection, improve systems integration and automation, and ensure that technology investments support organisational strategy, operational efficiency, service quality and business growth.

Key Accountabilities

ICT Strategy and Digital Transformation

- Develop and implement an ICT strategy aligned with ACS's business objectives and growth priorities.
- Provide strategic advice to the COO and senior management on technology investments, emerging technologies and digital transformation opportunities.
- Identify opportunities to automate manual processes, improve workflows and enhance service delivery through technology.
- Develop and maintain an ICT roadmap covering infrastructure, applications, systems integration, cybersecurity and business continuity.
- Evaluate and recommend appropriate technology solutions that support business scalability and operational efficiency.

Systems Development and Business Applications

- Oversee the implementation, maintenance and optimisation of business applications supporting claims processing, pre-authorisation, member management, provider administration and reporting.
- Ensure effective integration between business systems to improve information flow, accuracy and operational visibility.
- Drive the automation of manual processes, including claims tracking, reconciliations, reporting and workflow management.
- Oversee the management, availability and continuous improvement of member and provider portals and other digital service channels.

- Work with business stakeholders and technology vendors to define system requirements, manage implementations and resolve application issues.
- Ensure systems are fit for purpose, user-friendly, scalable and aligned with business needs.

Infrastructure and Service Delivery

- Oversee the management and maintenance of ICT infrastructure, including networks, servers, cloud services, end-user devices, communication systems and business applications.
- Ensure the availability, performance, reliability and security of ICT systems.
- Establish ICT service standards, incident management procedures and service-level agreements.
- Oversee the ICT helpdesk, ensuring timely resolution of user requests, technical incidents and system failures.
- Manage technology assets, licences, configurations and lifecycle replacements.
- Ensure adequate ICT resources, tools and support arrangements are available to employees.

Cybersecurity, Data Protection and Information Governance

- Develop and implement ICT security policies, standards and controls to protect ACS's information assets.
- Establish appropriate access controls, user authentication, privileged access management and system monitoring.
- Protect confidential member, provider, payer and scheme information against unauthorised access, loss, disclosure or misuse.
- Ensure ICT practices comply with applicable data protection legislation, regulatory requirements, contractual obligations and internal policies.
- Conduct periodic reviews of system vulnerabilities, security risks and access rights.
- Coordinate cybersecurity awareness, incident response and investigation of technology-related security breaches.
- Maintain appropriate audit trails, system logs and information retention controls.

Business Continuity and Disaster Recovery

- Develop, implement and periodically test ICT business continuity and disaster recovery plans.
- Ensure regular backups, secure backup storage and tested data restoration procedures.
- Establish system recovery priorities, recovery time objectives and recovery point objectives in consultation with business stakeholders.
- Coordinate responses to system outages, cyber incidents and other technology disruptions.
- Ensure critical business systems can be restored within agreed recovery timelines.
- Document incidents, corrective actions and lessons learned to strengthen operational resilience.

Data Management, Reporting and Analytics

- Establish appropriate standards for data integrity, data quality, accessibility and security.
- Support the development of reliable management dashboards and operational reports.
- Work with business teams to improve data availability for claims performance monitoring, service turnaround analysis, utilisation reporting and operational decision-making.
- Promote appropriate use of business intelligence, analytics and automation tools.
- Ensure data interfaces, reporting processes and system outputs are accurate, consistent and reliable.

Vendor and Contract Management

- Manage relationships with ICT service providers, software vendors, telecommunications providers and technology partners.
- Define technical requirements, service expectations and performance standards for external providers.

- Monitor vendor performance against contractual obligations and agreed service levels.
- Evaluate technology proposals and conduct technical assessments to support procurement decisions.
- Negotiate service arrangements and recommend cost-effective solutions.
- Ensure appropriate due diligence, confidentiality provisions, security requirements and exit arrangements are in place for technology vendors.

ICT Budgeting and Resource Management

- Develop and manage the annual ICT budget in consultation with the COO and Finance function.
- Monitor expenditure, technology costs and budget utilisation.
- Prepare business cases for ICT investments, demonstrating expected benefits, costs, risks and value for money.
- Optimise technology expenditure while maintaining appropriate service quality, security and resilience.
- Oversee ICT asset management, licence renewals and resource allocation.
- Lead, coach and develop ICT staff to build technical capability, accountability and service orientation.

Risk Management, Audit and Compliance

- Maintain an ICT risk register and implement appropriate mitigation measures.
- Coordinate ICT audits, vulnerability assessments, compliance reviews and closure of audit findings.
- Ensure technology changes are properly assessed, tested, approved and documented before implementation.
- Establish change management, configuration management and system documentation standards.
- Report significant ICT risks, incidents, service disruptions and remediation progress to the COO.
- Promote a culture of accountability, continuous improvement and responsible technology use.

Key Performance Indicators

- **Systems availability:** Achievement of approved uptime targets for critical business systems.
- **Incident resolution:** Compliance with agreed response and resolution times for ICT incidents and service requests.
- **Cybersecurity:** Timely resolution of identified vulnerabilities and implementation of approved security controls.
- **Data protection:** Compliance with information security and data protection requirements, including timely reporting and management of incidents.
- **Digital transformation:** Delivery of approved ICT projects and automation initiatives within agreed timelines and budgets.
- **Systems integration:** Successful implementation of prioritised integrations and reduction of manual data handling.
- **Business continuity:** Completion of scheduled backups, recovery tests and disaster recovery exercises.
- **ICT budget management:** Expenditure maintained within approved budgets, subject to authorised variations.
- **Vendor performance:** Compliance with agreed service-level agreements and timely resolution of vendor-related issues.
- **User satisfaction:** Achievement of agreed internal ICT service satisfaction targets.
- **Audit and compliance:** Timely closure of assigned ICT audit findings and risk remediation actions.
- **Project delivery:** Achievement of agreed milestones, quality standards and business benefits for ICT projects.

Qualifications

- Bachelor's degree in Information Technology, Computer Science, Information Systems, Software Engineering or a related field from a recognised institution.
- A relevant master's degree in Information Technology, Information Systems, Cybersecurity, Business Information Systems or Technology Management will be an added advantage.
- Professional certification in one or more relevant areas, such as ITIL, COBIT, CISSP, CISM, CISA, cloud technologies or project management, will be an advantage.
- Relevant training in information security, data protection, enterprise systems or IT service management will be desirable.

Experience

- At least eight (8) years of relevant ICT experience, including a minimum of three (3) years in a management or leadership role.
- Demonstrable experience managing ICT infrastructure, enterprise applications, cybersecurity, systems integration and technology service delivery.
- Experience implementing or managing business systems in healthcare, insurance, health financing, claims administration or another regulated environment will be an advantage.
- Proven experience leading ICT projects, managing technology vendors and budgets, and delivering systems improvements.
- Experience in cloud services, business continuity, disaster recovery, data management and information security.
- Demonstrated ability to translate business requirements into practical, scalable technology solutions.

Core Competencies

Technical

- ICT strategy development and execution
- Enterprise systems and application management
- Infrastructure, networks and cloud computing
- Cybersecurity and information security governance
- Data protection and information governance
- Systems integration, automation and digital transformation
- IT service management and incident resolution
- Business continuity and disaster recovery
- ICT risk management, audit and regulatory compliance
- Technology project, vendor and budget management
- Data analytics, business intelligence and management reporting

Leadership and Behavioural

- **Strategic thinking:** Aligns technology priorities with business strategy and future organisational needs.
- **Accountability:** Takes ownership of ICT performance, commitments, risks and outcomes.
- **Innovation:** Identifies practical opportunities to improve services and automate processes.
- **Problem-solving:** Diagnoses complex technical and operational challenges and implements sustainable solutions.
- **Communication:** Explains technical issues and recommendations clearly to non-technical stakeholders.

- **Stakeholder management:** Builds effective working relationships across business functions and with external partners.
- **People leadership:** Develops team capability, promotes collaboration and maintains high service standards.
- **Integrity and confidentiality:** Handles sensitive information responsibly and exercises sound professional judgement.
- **Change leadership:** Supports technology adoption and guides employees through systems and process changes.

How to apply

Send your CV and cover letter to hr@acs.co.ke with "Senior Manager - ICT" in the subject line by **2 November 2026**.