

# VACANCY

make the connection  
**mtc**

The positive growth at MTC, Namibia's leading telecommunications company, now warrants appointment in the following vacancy:

## Manager: IT Governance, Risk & Cybersecurity (D5)

The incumbent will report to the: **Chief Technology Information Office**

### Job Competencies Include:

The role is responsible for managing and overseeing MTC's ICT governance by ensuring that technology investments, operations, and risks are managed in alignment with business objectives, compliance requirements, standards and internal control. The role oversees the IT risk management, internal audits, cybersecurity governance, policy compliance, and provides independent assurance to executive and board-level stakeholders.

- Manage and define strategic goals and objectives for the Governance / IT Audit, Risk & Cybersecurity team in alignment with the overall business strategy.
- Develop, implement, and maintain a robust IT governance framework aligned with ISO standards and organisational strategic goals.
- Develop and operationalise the IT risk management framework, integrated with the enterprise risk management (ERM) strategy.
- Develop and own the technology risk appetite statement, translating it into measurable control objectives for critical infrastructure.
- Establish a Third-Party & Supply Chain Cyber Risk program to assess and monitor the security posture of key vendors and partners.
- Implement and chair a formal Technology Risk Committee to provide executive-level oversight and reporting on technology and cyber risk.
- Facilitate cross-functional engagement with IT operations, business units, compliance, legal, audit, and vendors to support a unified governance approach.
- Serve as the primary liaison with 3<sup>rd</sup> party/vendors and regulators on IT and cyber resilience, examinations, and mandatory reporting.
- Direct the security architecture review process for all new projects, digital products, and network technologies before launch.
- Ensure the organisation meets all technology-related regulatory requirements (e.g., POPIA, GDPR, sector-specific laws).
- Proactively identify, assess, document, and monitor technology risks (strategic, operational, cybersecurity, compliance, etc.).
- Build and lead a high-performing, technically skilled team capable of operating under strict regulatory scrutiny and in high-pressure incident scenarios.
- Promote a culture of cybersecurity through awareness campaigns, simulated attacks, and continuous education.
- Manage key performance indicators(KPIs) to track the effectiveness of Governance /IT Audit, Risk & Cybersecurity processes and systems.
- Champion the integration of Governance, Risk & Compliance (GRC) automation tools to provide real-time risk dashboards and streamline control testing.
- Proactively identify, assess, document, and monitor technology risks (strategic, operational, cybersecurity, compliance, etc.).
- Design and oversee a continuous controls monitoring (CCM) program for critical network and IT assets to detect control failures in real-time.
- Identify and implement improvements in business processes through technology solutions.

### Qualifications and Personal Competencies:

- Bachelor's degree in Cybersecurity, Computer Science, Information Technology, Telecommunications, or a related field.
- Minimum of 8 years' of progressive experience in IT, with a focus on governance, risk, compliance, and/or cybersecurity.
- Minimum of 5 years' of hands-on experience in a combination of IT governance, enterprise risk management, cybersecurity operations, and IT audit.
- Minimum of 3 years' in a managerial or team lead role.
- Proven 3 years' experience working in a highly regulated environment (Telecommunications, Financial Services/Banking, or similar).
- Experience with sector-specific regulators is a distinct advantage.
- Minimum of 3 years' of demonstrated experience in managing, controlling, and reporting on departmental budgets and capital expenditures.
- Cybersecurity Certification: CISM (Certified Information Security Manager), CISSP (Certified Information Systems Security Professional), Certified in the Governance of Enterprise IT (CGEIT) or CISA (Certified Information Systems Auditor).
- Additional certifications such as CRISC (Certified in Risk and Information Systems Control), ISO 27001 Lead Implementer/Auditor, COBIT Foundation/ Design & Implementation, or TOGAF.
- Proficiency in Cybersecurity architecture and controls.
- Strong people management skills and decision-making skills.
- Highly analytical mindset with strong attention to detail.
- Must have a valid driver's license.
- Must be a Namibian citizen or have permanent residency.

**Application closing date: Wednesday, 18 February 2026**

Submissions should contain a comprehensive CV, supported by a motivation (cover) letter, and Qualifications and should be addressed as follows:

Apply via the recruitment site: [https://jobopportunities.net/jobs\\_search.aspx](https://jobopportunities.net/jobs_search.aspx)

**No Hand delivered applications will be accepted.**

**NB: Only short-listed candidates will be contacted, and no CVs or documents will be returned.**

\* Previously disadvantaged people are encouraged to apply. MTC is an equal opportunities employer and offers a competitive remuneration package to the successful candidate.



Scan  
to apply



[mtc.com.na](https://mtc.com.na)

