

ZAMBIA DIGITAL READINESS

12-Month Sector Roadmap

Cybersecurity, Cloud & AI Readiness



Telecommunications



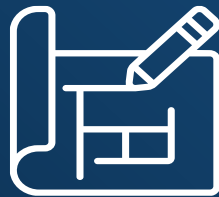
Purpose Of This Roadmap

This roadmap supports the Zambia Market Entry Webinar by giving Telecommunications attendees a practical plan to assess and advance digital readiness over the next 12 months. It is an educational and planning resource, not a sales proposal.



Benchmark

Locate your organisation on the
Basic → Standardized →
Rationalized → Dynamic model.



Plan

Use quarterly milestones as a
checklist, adapted to your size
and starting point.

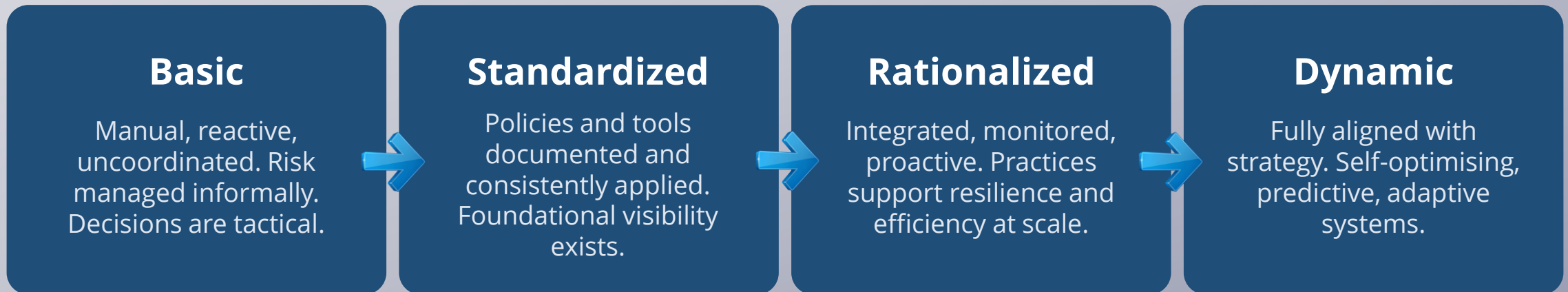


Track

Apply the KPIs as a basis for
internal targets once a baseline
is set.

The Maturity Model

A four-stage model adapted from Microsoft's Business Productivity and Core Infrastructure Optimization frameworks — applied consistently across cybersecurity, cloud, data/AI, and governance.



This roadmap is designed to move priority dimensions at least one stage forward within 12 months — not to assume a single leap to Dynamic.

Cybersecurity & Resilience

Cloud Readiness & Infrastructure

Data & AI Adoption

Governance, People & Process

Telecommunications

CURRENT MATURITY SNAPSHOT

Network operations and core connectivity are generally Standardized to Rationalized, while customer data governance, cloud-native platforms, and AI-driven network optimisation often remain Basic to Standardized.

MATURITY PATHWAY — KEY DIMENSION

Cybersecurity & Resilience

Basic

Network security focused on perimeter firewalls; limited visibility into enterprise and mobile money platforms; informal incident handling.

Standardized

Network operations centre (NOC) with basic security monitoring; documented incident response for network outages and major security events; periodic security audits.

Rationalized

Integrated NOC/SOC with correlated network and security monitoring; mature DDoS protection for customer-facing services; regular third-party security assessments of mobile money and enterprise platforms.

Dynamic

AI-assisted threat detection across network and application layers; automated mitigation for large-scale attacks; continuous assurance testing aligned to national critical infrastructure requirements.

TELECOMMUNICATIONS

Cloud Readiness & Infrastructure

Basic

Core network functions largely on dedicated hardware; limited virtualization; manual provisioning for new services.

Standardized

Virtualised core network functions; hybrid cloud adopted for IT systems (billing, CRM, support); documented backup and DR for critical platforms.

Rationalized

Network functions virtualization (NFV) and software-defined networking adopted for key services; enterprise and consumer digital platforms run on scalable cloud infrastructure; automated failover for critical services.

Dynamic

Cloud-native, API-driven network and service architecture; auto-scaling to meet demand spikes (events, mobile money peaks); infrastructure-as-code with continuous compliance monitoring.

TELECOMMUNICATIONS

Data & AI Adoption



Basic



Customer and network performance data siloed across billing, network, and customer service systems; no formal AI use.

Standardized



Centralised reporting for network performance and customer experience; initial data protection policy; pilot AI use cases for customer service or fraud detection in mobile money.

Rationalized



AI-enabled network optimisation (capacity planning, fault prediction); fraud detection embedded in mobile money platforms; data governance covering customer privacy and lawful interception requirements.

Dynamic

Predictive network maintenance and self-optimising networks; AI-driven personalisation of enterprise and consumer offers; real-time fraud and anomaly detection across all digital financial services.

TELECOMMUNICATIONS

Governance, People & Process

Basic

Security and digital risk managed within IT/network teams with limited executive visibility; ad hoc vendor management.

Standardized

Digital and security risk reported to senior technology leadership; structured vendor and partner risk assessments; baseline technical certification programmes.

Rationalized

Executive-level digital resilience committee; structured career and certification pathways for network, cloud, and security teams; mature change management for network and platform upgrades.

Dynamic

Digital resilience integrated into enterprise strategy and regulatory engagement; continuous technical upskilling aligned to emerging technologies (5G, NFV, AI); cross-industry collaboration on national digital infrastructure resilience.

TELECOMMUNICATIONS

12-Month Quarterly Roadmap

Q1 (Months 1-3)

Assess & Stabilise

- Conduct a joint network and security readiness assessment covering core network, mobile money, and enterprise platforms.
- Establish integrated visibility between NOC and security monitoring where these currently operate separately.
- Inventory customer and network data sources; identify lawful interception and data protection obligations.
- Define executive-level reporting on digital resilience and security posture.

Q2 (Months 4-6)

Strengthen Foundations

- Deploy or upgrade DDoS protection and security monitoring for customer-facing digital and mobile money platforms.
- Migrate billing, CRM, and support systems to a hybrid cloud environment with documented backup and DR.
- Pilot an AI use case for fraud detection in mobile money or for customer service automation.
- Conduct a third-party security assessment of mobile money and key enterprise platforms.

Q3 (Months 7-9)

Scale & Integrate

- Adopt network functions virtualization or software-defined approaches for at least one critical network domain.
- Move validated AI fraud detection or network optimisation pilots into production with monitoring.
- Establish a data governance framework covering customer privacy, data classification, and retention.
- Run a coordinated incident response exercise spanning network and security teams.

Q4 (Months 10-12)

Optimise & Govern

- Implement automated failover and auto-scaling for at least one critical customer-facing platform.
- Formalise an executive-level digital resilience committee with quarterly review of network, security, and AI initiatives.
- Expand AI-enabled fault prediction or capacity planning across the core network.
- Publish a 12-month digital readiness review and define year-two priorities, including 5G or NFV roadmap alignment.

KEY PERFORMANCE INDICATORS

Indicative 12-month targets. Establish baselines during Q1 assessment activities.

KPI / METRIC	12 MONTH TARGET
01 Network and security incident detection time	Reduce by 35% from baseline by Month 12
02 Mobile money fraud detection rate (true positives)	Improve by 25% by Month 9
03 % of critical platforms with automated failover/DR	From baseline to 75% by Month 12
04 Customer-facing platform uptime (SLA-critical services)	Maintain or improve to 99.9% by Month 12
05 % of customer data classified under governance framework	100% of high-sensitivity data by Month 9
06 Number of AI use cases in production (network or fraud)	At least 2 by Month 12
07 Technical staff with current cloud/security certifications	Increase by 30% by Month 12

TELECOMMUNICATIONS

Next Steps

Digital readiness is not a one-time project but an ongoing discipline. For Telecommunications, the priority is to move further along in governance, data, and AI oversight to match the pace of technology adoption.

The path forward follows the same pattern:

1.

Assess
honestly

2.

Stabilise the
foundations

3.

Scale
deliberately

4.

Govern
continuously

This roadmap is offered as a starting point for that conversation — within your organisation, across industry peers, and as part of the dialogue the Zambia Market Entry Webinar aims to convene.