ISACA
Accra Chapter

LANCASTER KUMASI CITY HOTEL, KUMASI

Securing the Algorithm: AI Risks and Cybersecurity Challenges in Africa’s Financial Sector

Presentation By: Desmond Israel Esq. CISSP, CIPM, CCT, CC

PROFILE

- Partner (Cyberlaw and Technology Practice), AGNOS Legal Company
- Lecturer, GIMPA Law School
- Lead Consultant, Information Security Architects Ltd
- Training Consultant, National Banking College
- Non-Executive Director, Zerone Analytiqs (Canada)
- Member, EC-Council BETA Testing Committee (United States of America)
- Volunteer, ISC2 Exam Development
- Research Lead, XRSI Guardian Safety Framework (California)
- Former Research Fellow, Center for AI and Digital Policy (Washington DC)
- Alumni LLM'23, The George Washington Law School (Washington DC)

AGENDA

- AI Strategy Trends
- AI in Africa’s Financial Sector
- AI-Ops in Finance
- Cyber Threats in AI Systems
- Mapping the Risk Landscape in Africa
- Securing the AI Pipeline
- Policy & Regulatory Governance
- Recommendations

AI STRATEGY TRENDS

Full-Stack Integrators believe that controlling the entire AI value chain—from silicon to consumer applications—creates insurmountable competitive advantages through synergy and integration.

These companies accept the complexity and capital requirements of competing across multiple layers in exchange for the potential to dominate entire ecosystems.

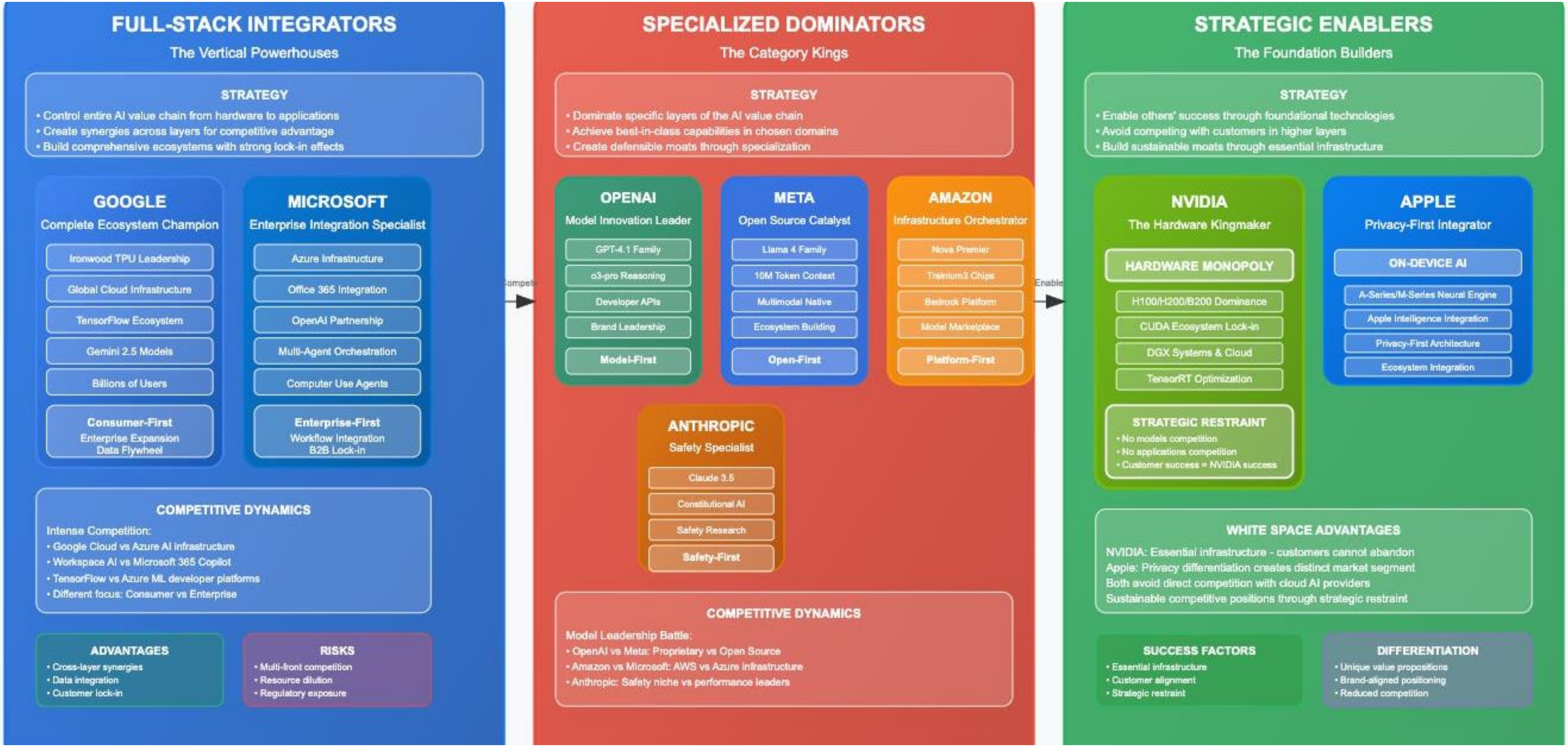
Specialized Dominators focus on achieving category leadership in specific layers of the AI stack, whether models, infrastructure, or platforms.

These companies bet that depth beats breadth, and that world-class capabilities in focused areas create more value than mediocre performance across many.

Strategic Enablers position themselves as essential infrastructure providers that enable others' success rather than competing with potential customers.

These companies have discovered that the most profitable position in a gold rush might be selling shovels rather than mining for gold.

The Three Strategic Archetypes



FULL-STACK INTEGRATORS

The Vertical Powerhouses

STRATEGY

- Control entire AI value chain from hardware to applications
- Create synergies across layers for competitive advantage
- Build comprehensive ecosystems with strong lock-in effects

GOOGLE

Complete Ecosystem Champion

- Ironwood TPU Leadership
- Global Cloud Infrastructure
- TensorFlow Ecosystem
- Gemini 2.5 Models
- Billions of Users

Consumer-First
Enterprise Expansion
Data Flywheel

MICROSOFT

Enterprise Integration Specialist

- Azure Infrastructure
- Office 365 Integration
- OpenAI Partnership
- Multi-Agent Orchestration
- Computer Use Agents

Enterprise-First
Workflow Integration
B2B Lock-in

COMPETITIVE DYNAMICS

Intense Competition:

- Google Cloud vs Azure AI infrastructure
- Workspace AI vs Microsoft 365 Copilot
- TensorFlow vs Azure ML developer platforms
- Different focus: Consumer vs Enterprise

ADVANTAGES

- Cross-layer synergies
- Data integration
- Customer lock-in

RISKS

- Multi-front competition
- Resource dilution
- Regulatory exposure

SPECIALIZED DOMINATORS

The Category Kings

STRATEGY

- Dominate specific layers of the AI value chain
- Achieve best-in-class capabilities in chosen domains
- Create defensible moats through specialization

OPENAI

Model Innovation Leader

- GPT-4.1 Family
- o3-pro Reasoning
- Developer APIs
- Brand Leadership

Model-First

META

Open Source Catalyst

- Llama 4 Family
- 10M Token Context
- Multimodal Native
- Ecosystem Building

Open-First

AMAZON

Infrastructure Orchestrator

- Nova Premier
- Trainium3 Chips
- Bedrock Platform
- Model Marketplace

Platform-First

ANTHROPIC

Safety Specialist

- Claude 3.5
- Constitutional AI
- Safety Research

Safety-First

COMPETITIVE DYNAMICS

Model Leadership Battle:

- OpenAI vs Meta: Proprietary vs Open Source
- Amazon vs Microsoft: AWS vs Azure infrastructure
- Anthropic: Safety niche vs performance leaders

STRATEGIC ENABLERS

The Foundation Builders

STRATEGY

- Enable others' success through foundational technologies
- Avoid competing with customers in higher layers
- Build sustainable moats through essential infrastructure

NVIDIA

The Hardware Kingmaker

HARDWARE MONOPOLY

- H100/H200/B200 Dominance
- CUDA Ecosystem Lock-in
- DGX Systems & Cloud
- TensorRT Optimization

STRATEGIC RESTRAINT

- No models competition
- No applications competition
- Customer success = NVIDIA success

APPLE

Privacy-First Integrator

ON-DEVICE AI

- A-Series/M-Series Neural Engine
- Apple Intelligence Integration
- Privacy-First Architecture
- Ecosystem Integration

WHITE SPACE ADVANTAGES

NVIDIA: Essential infrastructure - customers cannot abandon
Apple: Privacy differentiation creates distinct market segment
Both avoid direct competition with cloud AI providers
Sustainable competitive positions through strategic restraint

SUCCESS FACTORS

- Essential infrastructure
- Customer alignment
- Strategic restraint

DIFFERENTIATION

- Unique value propositions
- Brand-aligned positioning
- Reduced competition

AI IN AFRICA’S FINANCIAL SECTOR

Accelerating AI Adoption

Fintech & Banking Pioneers: AI-driven services are emerging rapidly in digital lending, customer onboarding (eKYC), credit scoring, and fraud detection across Nigeria, Kenya, Ghana, and South Africa.

Key Drivers: Mobile penetration, fintech investments, and digital public infrastructure (DPI) such as national ID systems and payment rails (e.g., Ghana’s GhIPSS, Nigeria’s NIBSS).

Strategic Opportunities

Financial Inclusion: AI enables thin-file credit profiling using alternative data (e.g., telco usage, mobile money history), improving access for underserved segments.

Operational Efficiency: AI is optimizing risk modeling, regulatory compliance (e.g., RegTech in AML/CFT), and customer engagement via intelligent chatbots.

Cross-Border Potential: AfCFTA’s digital strategy envisions AI as a lever for integrated payment systems and financial services interoperability across African markets.

AI IN AFRICA'S FINANCIAL SECTOR

Digital Trust & Governance Challenges

Data Infrastructure Gaps: Inconsistent data quality, fragmented systems, and limited access to reliable financial data hinder AI deployment.

Privacy & Ethics Risks: Weak enforcement of data protection frameworks (e.g., limited uptake of GDPR-inspired local laws) raises concerns on consent, profiling, and fairness.

Cybersecurity Vulnerabilities: Central banks and FSIs report rising threats, including AI-powered fraud, requiring stronger cyber hygiene and threat intelligence mechanisms.

Institutional Responses

Central Bank Sandboxes: Countries like Ghana, Rwanda, and Nigeria are testing AI innovations under controlled regulatory environments.

Regional Harmonization: AfDB and Smart Africa are pushing for pan-African AI strategies aligned with financial stability, inclusion, and trust principles.

AI-OPS IN FINANCE

- **Core Use Case – Proven Application in Financial Operations**

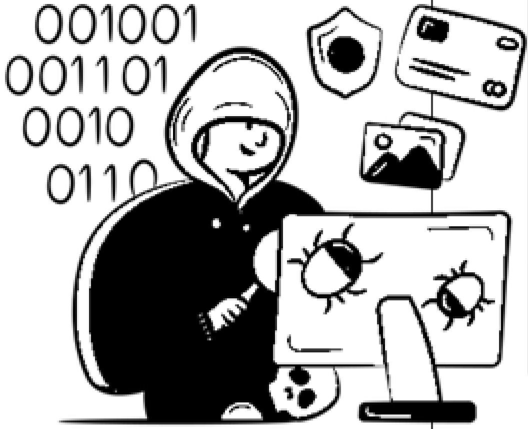
Fraud Detection **(Supervised Learning)**	**KYC Automation** **(Natural Language Processing + OCR)**	**Robo-Advisory** **(Predictive Analytics & NLP)**
Machine learning models flag anomalous transaction patterns in real-time using historical behavior data, geolocation, device signatures, and velocity checks.	AI extracts and verifies customer identity information (e.g., ID documents, proof of address) with automated decisioning, reducing onboarding time by over 70%.	AI-powered investment advisors provide personalized portfolio allocation based on risk appetite, income level, and market conditions.
Example: **Mastercard** uses AI models to scan 75 billion transactions annually with 99.5% **fraud detection accuracy** (source: Mastercard AI Labs).	*Example*: **Jumio** and **Onfido** use hybrid AI-human **KYC verification** in global fintech and neobank deployments.	*Example*: **Betterment** and African players like **Ndovu** use reinforcement learning to **rebalance portfolios** dynamically.

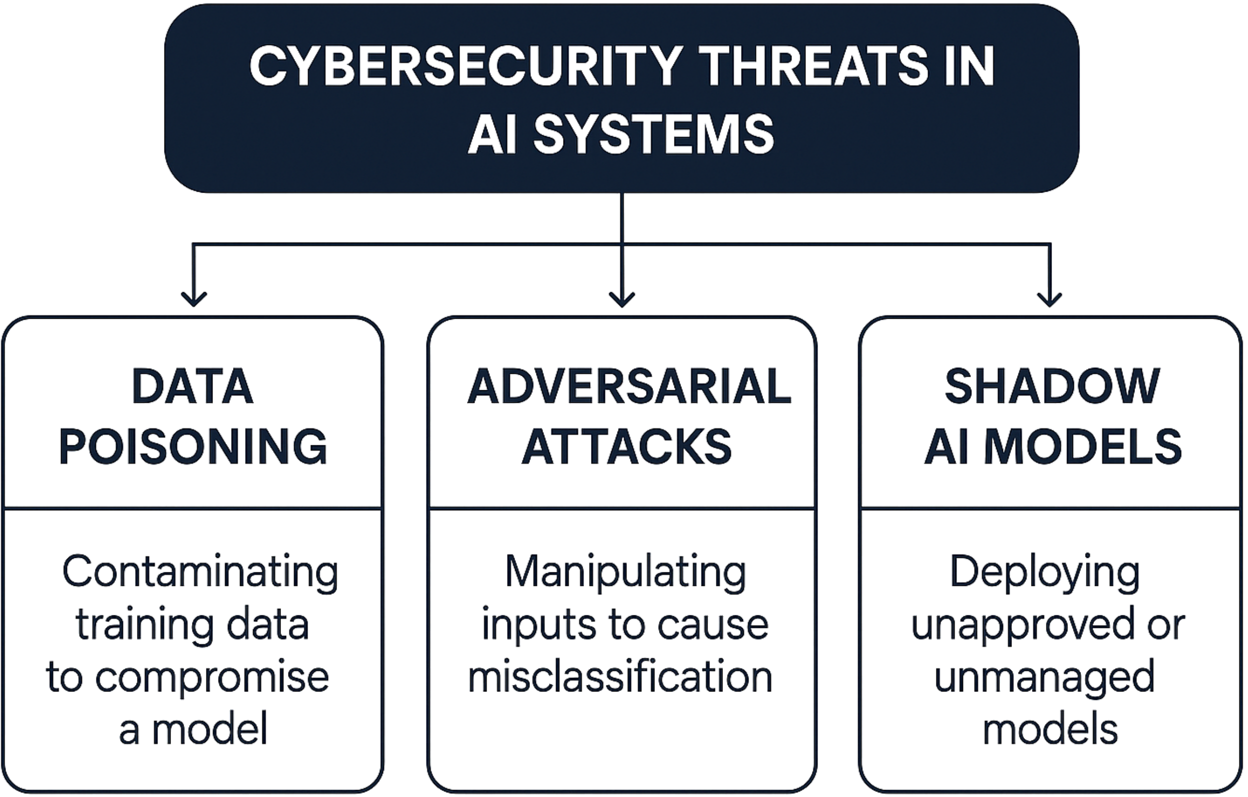
AI-OPS IN FINANCE

- **Key AI Risk Factors in Finance**

Model Bias **(Training Data Risk)**	**Opacity** **(Black-Box Decisions)**	**Expanded Attack Surfaces** **(Adversarial AI Risk)**
Algorithms trained on skewed datasets (e.g., urban vs rural income profiles) can embed systemic bias in credit scoring or fraud suspicion flags.	High-complexity models (e.g., deep neural networks) often lack explainability, undermining transparency obligations in financial services.	AI systems can be targeted via data poisoning, model inversion, or adversarial examples, leading to manipulated credit approvals or undetected fraud.
Regulatory Note: The Bank of Ghana and South Africa’s FSCA emphasize fairness audits for AI models.	*Compliance Implication*: EU AI Act and global regulators advocate for Explainable AI (XAI) in high-risk applications.	*Security Concern*: Gartner warns that by 2026, 30% of AI-enabled financial systems will be exploited via novel attack vectors without proper AI security protocols.

CYBER THREATS IN AI SYSTEMS





CYBERSECURITY THREATS IN AI SYSTEMS

DATA POISONING

Contaminating training data to compromise a model

ADVERSARIAL ATTACKS

Manipulating inputs to cause misclassification

SHADOW AI MODELS

Deploying unapproved or unmanaged models

CYBER THREATS IN AI SYSTEMS

Data Poisoning (Supply Chain Risk to Model Integrity)
Attackers introduce malicious data into training pipelines—polluting datasets to manipulate AI outputs, misclassify fraud, or embed backdoors.

Impact: Compromised AI models may approve fraudulent transactions or flag legitimate behaviour as suspicious.

Real-World Insight: Financial AI vendors increasingly face upstream risks from open-source training sets and third-party data brokers.

Response: Incorporate data validation gates and lineage tracing across model pipelines (NIST AI RMF SP 1270).

CYBER THREATS IN AI SYSTEMS

Adversarial Attacks (Input Manipulation for Misclassification)
Carefully crafted inputs cause AI models to make incorrect decisions—without obvious anomalies to human observers.

Financial Relevance: Slight alterations in transaction metadata or user behavior patterns can bypass fraud detection systems.

Key Threats: Evasion attacks (real-time fraud masking) and model inversion (reconstructing sensitive training data).

Mitigation: Deploy adversarial testing frameworks and robust model hardening techniques (e.g., adversarial training, differential privacy).

CYBER THREATS IN AI SYSTEMS

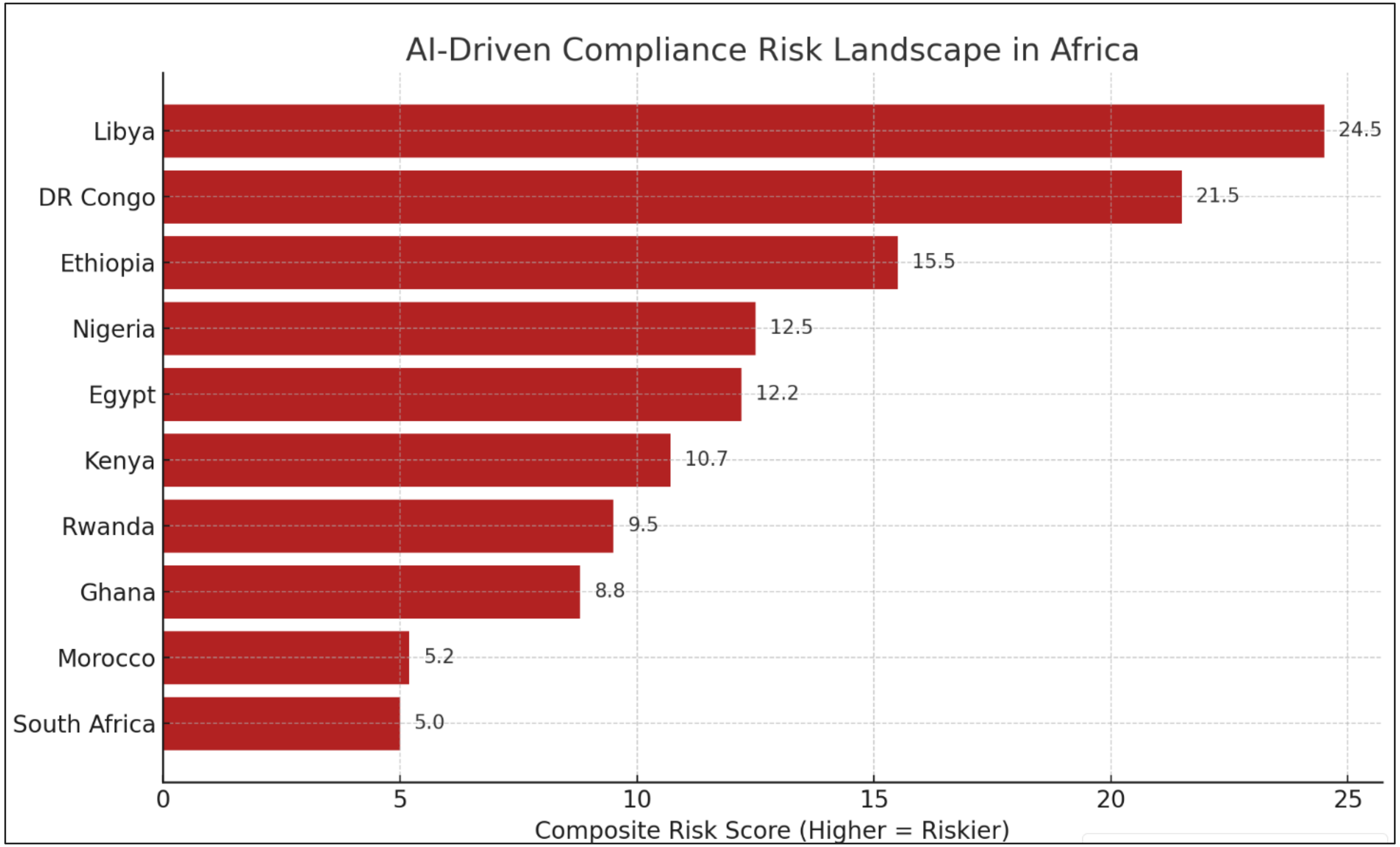
Shadow AI Models (Unauthorized or Rogue Deployments)
Unofficial or unmanaged AI models operated outside enterprise governance expose firms to unvetted risks.

Risk Context: Employees may deploy local AI models for analytics or decision support, bypassing oversight on data access, security, and compliance.

Regulatory Note: Shadow AI undermines explainability, auditability, and can breach sectoral data protection obligations (e.g., DPA2012, GDPR, Nigeria's NDPR).

Control Strategy: Implement AI asset inventories, zero-trust data access, and model usage logging per ISACA AI Governance Framework.

MAPPING THE RISK LANDSCAPE IN AFRICA



A **ranked bar chart** visualizing the **Composite Compliance Risk Score** across selected African countries. It illustrates which nations face greater systemic risk due to gaps in data protection, cybersecurity maturity, and AI readiness.

It combines **data protection laws**, **cybersecurity maturity**, and **AI readiness** from **ITU Global Cybersecurity Index**, **UNCTAD Data Protection Tracker**, or **ISACA Risk Maturity Models**.

MAPPING THE RISK LANDSCAPE IN AFRICA

Regulatory Gaps
While over 30 African countries have enacted data protection laws, enforcement remains fragmented and underfunded. Many Data Protection Authorities (DPAs) lack operational independence and investigative capacity.

Example: Ghana's Data Protection Commission (DPC) has limited prosecutorial power and relies heavily on public sector compliance by directive.

Infrastructural Weaknesses
Critical digital infrastructure (e.g., broadband, secure cloud, encryption key management) is unevenly deployed, particularly outside urban hubs. This undermines cybersecurity resilience and trusted AI deployment.

Insight: Only 39% of African countries have a national Computer Emergency Response Team (CERT) per ITU GCI (2023).

Talent Shortages
There is a regional deficit of skilled professionals in cybersecurity, AI governance, and compliance auditing. This exposes both public and private institutions to avoidable risk escalation.

Data Point: ISC^2 (2024) estimates a shortfall of over 150,000 cybersecurity professionals across Africa.

SECURING THE AI PIPELINE

Cyber Hygiene in AI/ML DevOps

Apply secure SDLC principles to model development lifecycles (data > training > deployment).

Enforce **data provenance checks**, version control (e.g., DVC), encrypted storage, and hardened containers.

Regularly validate **model behavior drift** and **baseline outputs** to detect anomalies post-deployment.

Vendor & Third-Party AI Model Risk

- Increasing use of external AI APIs (e.g., LLMs, fraud detection engines) exposes financial institutions to **opaque architectures** and **undisclosed training data**.
- Key risks: IP leakage, regulatory non-compliance (e.g., cross-border data transfer), and lack of explainability.
- Require **AI vendor disclosures** on model lineage, update cycles, and incident response SLAs.

MLOps + InfoSec Integration Checklist

- **DataOps**

Validate input sanitization, detect poisoned datasets

- **ModelOps**

Use adversarial testing & XAI tools for transparency

- **CI/CD Pipelines**

Sign all model artifacts; monitor for unauthorized changes

- **Runtime**

Log all model inferences; enforce RBAC & model firewalls

SECURING THE AI PIPELINE

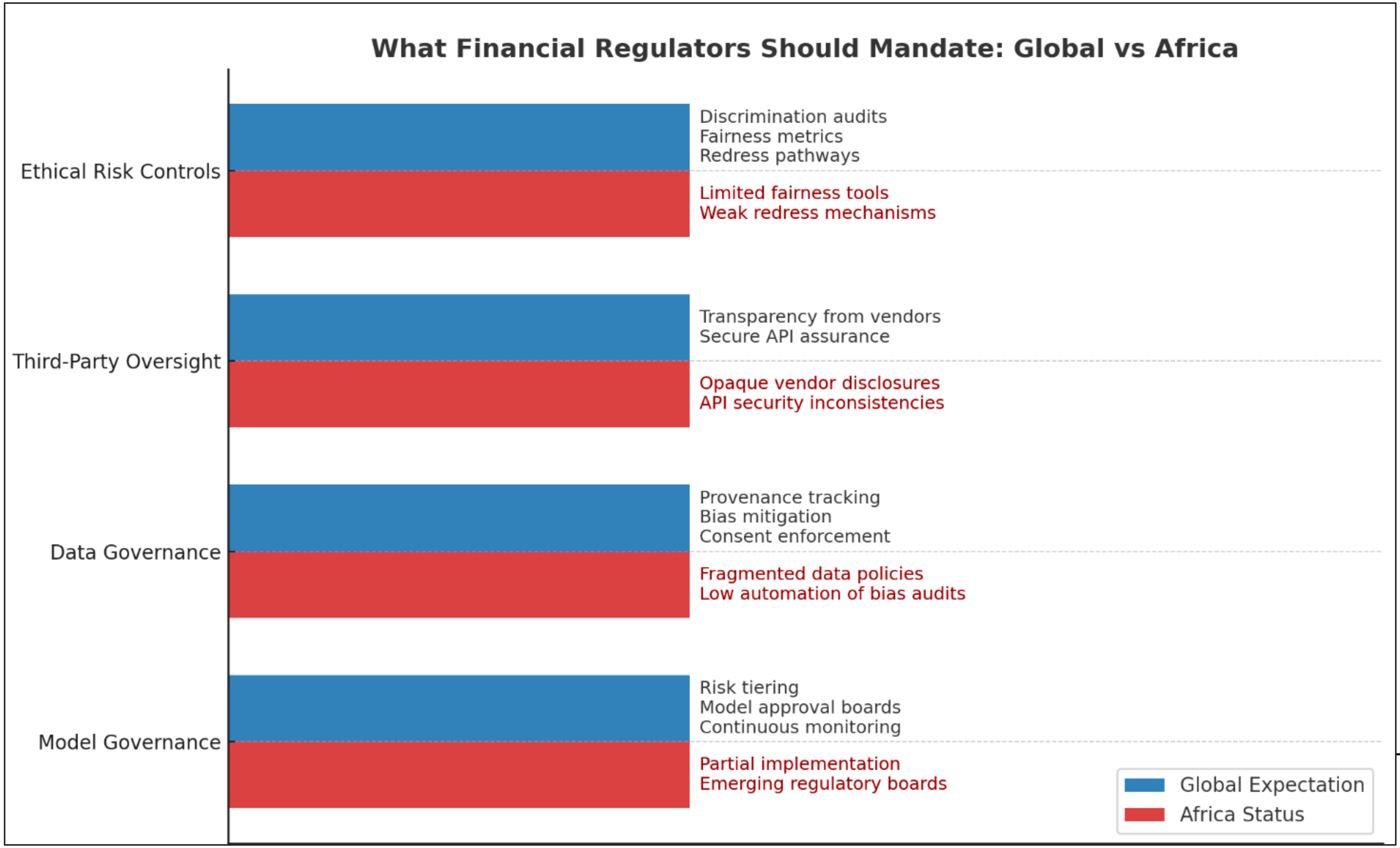
Continuous Threat Exposure Management (CTEM) for AI Security
CTEM enables **real-time, proactive security validation** across the AI stack—far beyond traditional static controls.

CTEM Validates Exposure To:

- **Adversarial Inputs**: Simulates inference-time attacks (e.g., evasion, perturbation) on models.
- **Pipeline Misconfigurations**: Detects insecure DevOps linkages, missing audit trails, weak privilege segregation.
- **Third-Party Toolchain Vulnerabilities**: Continuously scans SDKs, APIs, model registries, and orchestrators (e.g., Kubeflow, MLflow).
- **Emerging Regulatory or Threat Intelligence Feeds**: Auto-maps model behavior and governance to evolving compliance (e.g., EU AI Act, DPA/NDPA, Basel guidance on AI in risk).

ISACA's Role: Drive CTEM adoption as a control baseline in AI audit, GRC frameworks, and board-level oversight

POLICY & REGULATORY GOVERNANCE



What Financial Regulators Should Mandate: Global vs Africa

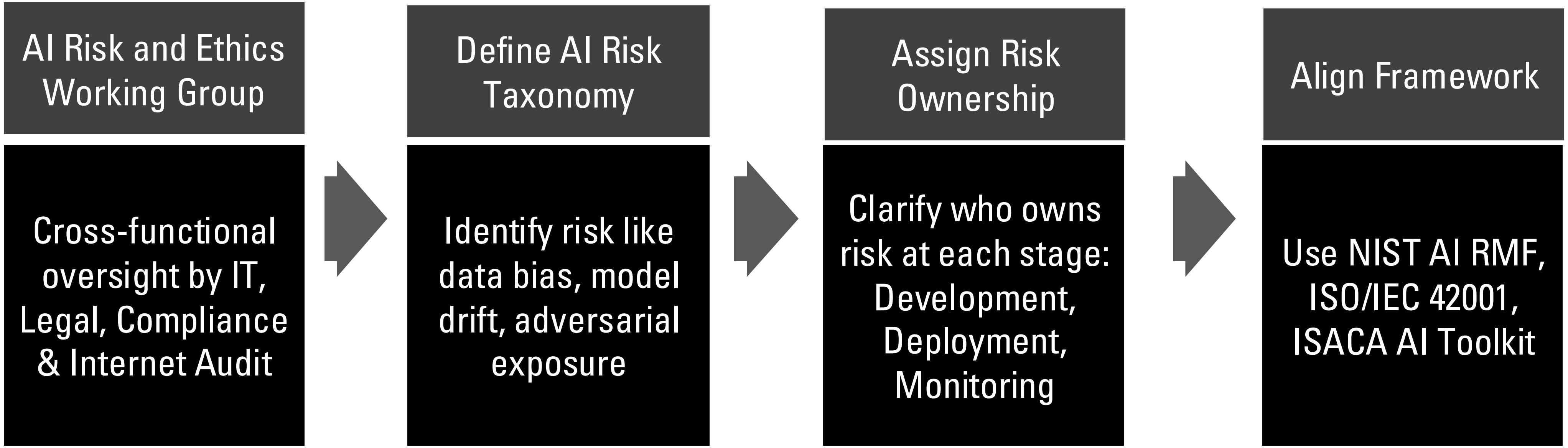
A graphical comparison of what financial regulators should mandate—**contrasting global expectations with the current African regulatory landscape** across four critical AI governance categories.

POLICY & REGULATORY GOVERNANCE

Auditability	Model Registry Requirements	Explainability Standards
Supervisory authorities must require that AI systems used in credit scoring, fraud detection, and customer profiling are **auditable end-to-end**—from data ingestion to final output.	Firms should operate a **centralized internal AI model registry** with metadata including purpose, owner, training data sources, regulatory impact level, and deployment context.	AI models used in decision-making must meet **context-appropriate explainability thresholds**, especially in high-stakes use cases like credit underwriting or fraud denial.
Best Practice: Maintain **model audit logs**, versioning history, and automated changelogs (aligned with Basel Committee principles on model risk).	*Global Trend*: Singapore’s MAS and UK's FCA encourage registries to enforce AI model lifecycle governance, including expiry policies and retraining thresholds.	*Example*: The EU AI Act requires that individuals affected by automated decisions receive “meaningful information about the logic involved.” *Regulatory Benchmark*: South Africa’s POPIA (s14) and Kenya’s DPA mandate human-readable rationales for automated decision-making.

RECOMMENDATION

- Institutionalize AI Risk Governance
- Implement Model Inventory & Classification Protocols (Risk level, Tiers etc)
- Integrate AI Controls into GRC Workflows (3PP DD/XDD)
- Foster CISO–Legal–Compliance Synergy (Regulatory exposure, monitoring)



AI Risk and Ethics Working Group

Cross-functional oversight by IT, Legal, Compliance & Internet Audit

Define AI Risk Taxonomy

Identify risk like data bias, model drift, adversarial exposure

Assign Risk Ownership

Clarify who owns risk at each stage: Development, Deployment, Monitoring

Align Framework

Use NIST AI RMF, ISO/IEC 42001, ISACA AI Toolkit

INTERACTIONS

THANK YOU

www.desmondisrael.legal