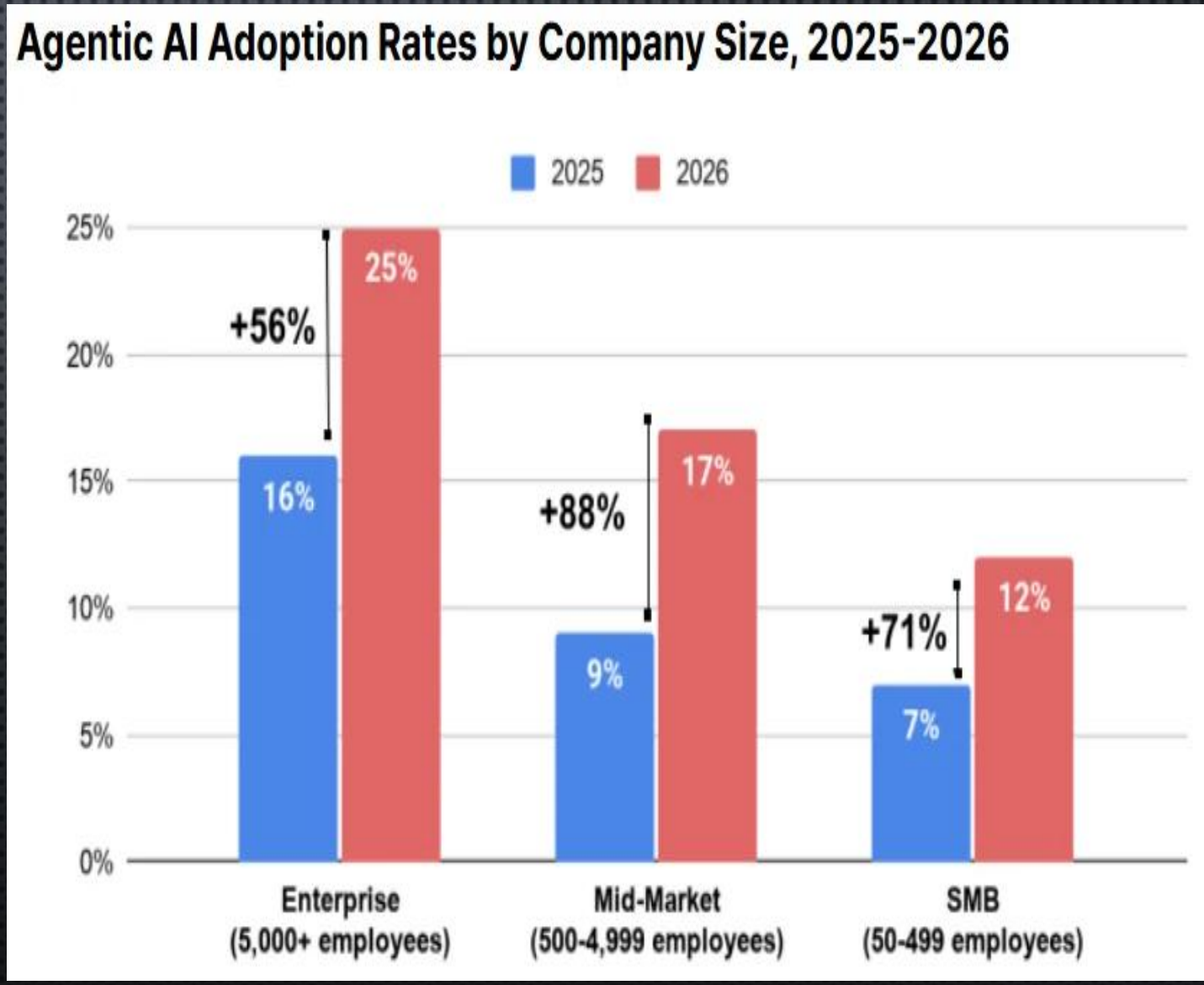
AGENTIC AI: THE NEW FINANCE PERSON

Dr Suraj Juddoo
s.juddoo@mdx.ac.mu

WHAT IS AGENTIC AI?

AGENTIC AI REFERS TO AI SYSTEMS CAPABLE OF:

- PERCEIVING CONTEXT
- MAKING DECISIONS
- PLANNING ACTIONS
- EXECUTING WORKFLOWS
- USING TOOLS AND APIS
- LEARNING FROM FEEDBACK
- ACTING WITH LIMITED HUMAN INTERVENTION

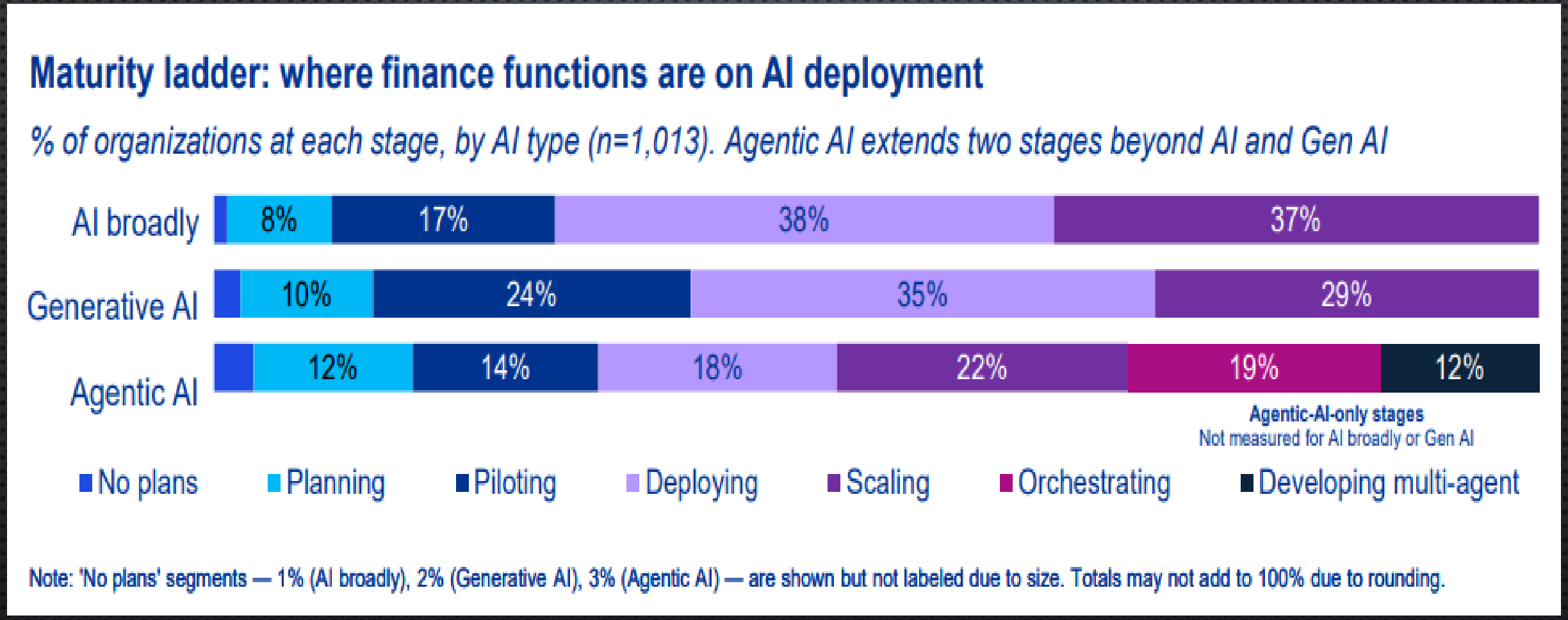


AGENTIC AI VS GENERATIVE AI

Feature	Generative AI	Agentic AI
Main function	Generate content	Execute goals
Autonomy	Low	Medium–High
Tool use	Limited	Extensive
Workflow execution	No	Yes
Decision-making	Assisted	Semi-autonomous
Examples	Chatbot	AI treasury operator

Finance Sector Example
Generative AI
"Summarise this loan application."
Agentic AI
Reviews documents → verifies data → checks sanctions → calculates risk → recommends approval.

AI IN FINANCE INDUSTRY



KPMG Global AI in Finance 2026 report

The financial sector is entering the "AI agent era"

Key Drivers

- Explosion of large language models
- Pressure for operational efficiency
- Rising compliance complexity
- Demand for real-time decisioning
- Increasing cyber and fraud threats
- Competition from fintechs and digital-native banks

Traditional AI	Predicts
Generative AI	Creates
Agentic AI	Acts autonomously

MULTI-AGENT FINANCE ECOSYSTEMS

Emerging Model

Instead of one AI:

- Compliance Agent
- Fraud Agent
- Treasury Agent
- Customer Service Agent
- Trading Agent
- Cybersecurity Agent

All collaborating in real time.

Example: AI-Powered Fraud Response

Traditional Process

- Detection → analyst review → escalation → action

Time:

Hours or days

Agentic AI Process

- Detect anomaly
- Cross-check identity
- Assess risk score
- Freeze account temporarily
- Notify customer
- Escalate to compliance

Time:

Seconds or minutes

QUANTIFIABLE BENEFITS

Area	Potential Impact
Compliance operations	Reduced manual workload
Fraud detection	Faster response times
Customer service	24/7 intelligent support
Treasury	Real-time optimization
Risk management	Continuous monitoring
Operational cost	Efficiency gains

RISKS OF AGENTIC AI

Operational	Governance	Cyber	Ethical
• Hallucinated actions • Wrong transactions • Autonomous errors	• Lack of explainability • Unclear accountability • Decision opacity	• Prompt injection • Tool abuse • Autonomous exploitation	• Bias • Discrimination • Financial exclusion

WHY GOVERNANCE IS HARDER THAN GENERATIVE AI

Challenge	Why Difficult
Accountability	Who is responsible?
Monitoring	Continuous behavior
Auditability	Dynamic decisions
Control	Agents evolve
Security	API access creates attack surface

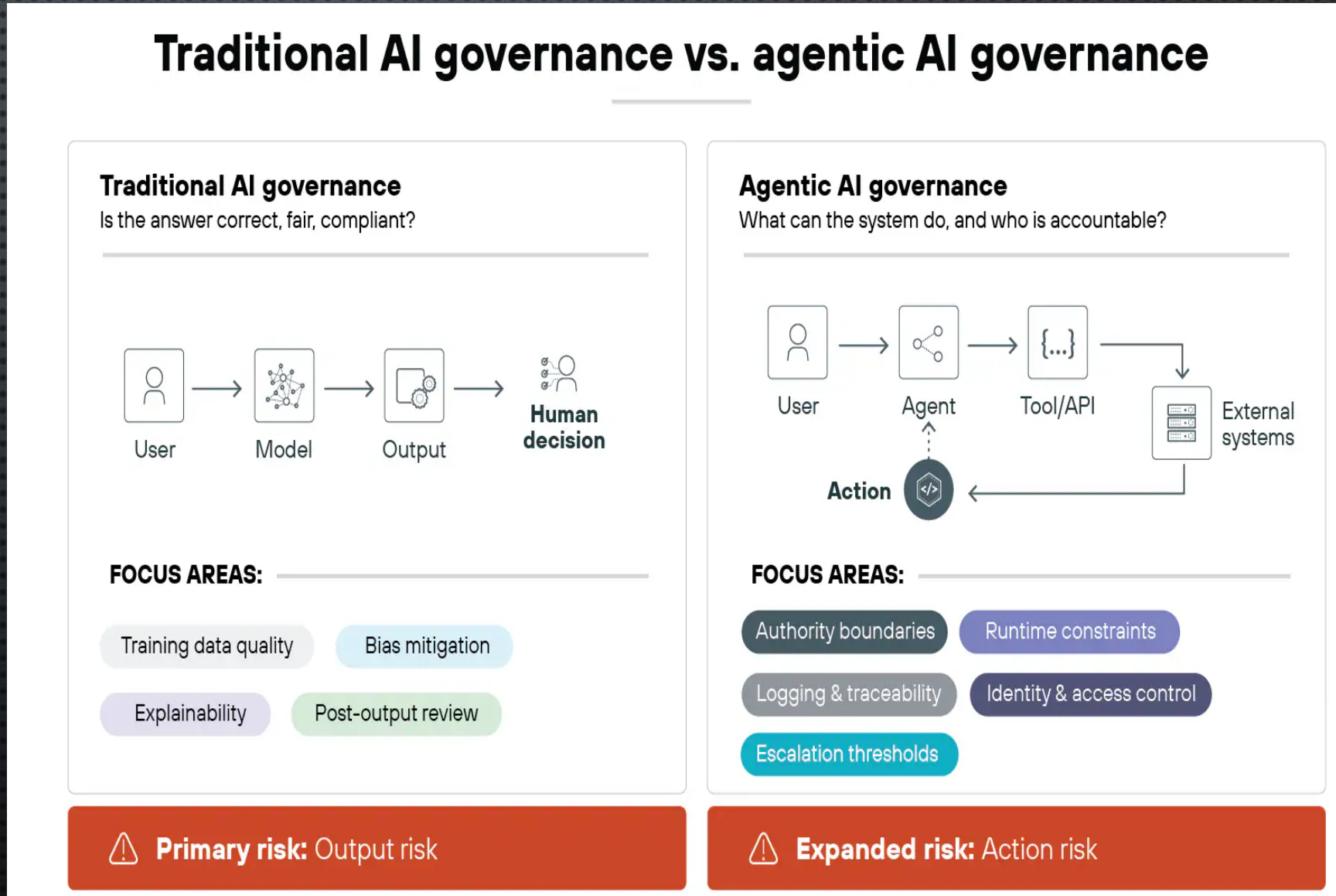
AGENTIC AI GOVERNANCE FRAMEWORK

Human Oversight	Explainability	Risk Classification	Security Controls	Regulatory Compliance
▪ Human-in-the-loop controls ▪ Escalation triggers	• Traceable reasoning • Action logging	• High-risk vs low-risk agents	• API restrictions • Sandboxing • Access management	• Data privacy • Financial regulations • Model governance

GLOBAL REGULATORY DIRECTION

TRENDS

- AI RISK GOVERNANCE
- MODEL ACCOUNTABILITY
- THIRD-PARTY AI OVERSIGHT
- CYBER RESILIENCE
- TRANSPARENCY OBLIGATIONS



HUMAN ROLES WILL CHANGE

Traditional Role	Future Role
Compliance analyst	AI compliance supervisor
Fraud investigator	AI investigation orchestrator
Trader	AI strategy controller
Auditor	AI governance auditor

Strategic Questions for Financial Institutions

Key Executive Questions

1. Which processes should remain human-led?
2. What level of autonomy is acceptable?
3. How do we audit AI actions?
4. Who owns AI decisions?
5. How do we secure AI agents?
6. How do regulators supervise autonomous systems?

Suggested Governance Model

"Three Lines of Defense" for Agentic AI

First Line

Business units operating AI agents

Second Line

Risk & compliance oversight

Third Line

Independent audit & validation

Future Outlook

What May Happen Next

- Autonomous digital banks
- AI-managed portfolios
- Self-healing cyber defence
- Real-time regulatory reporting
- AI-to-AI financial negotiations
- Autonomous compliance operations

Recommended Strategic Roadmap

Phase 1 — AI Readiness

- Data governance
- Infrastructure modernization
- AI literacy

Phase 2 — AI Assistance

- Copilots
- Workflow automation

Phase 3 — Controlled Agency

- Semi-autonomous agents
- Human oversight

Phase 4 — Autonomous Operations

- Full orchestration
- Continuous governance

QUESTIONS