



Agentic AI: Emerging risks and control strategies

May 2025



The better the question. The better the answer. The better the world works.



Shape the future
with confidence

Contents



1

Introduction to
Agentic AI

2

Agentic AI
adoption

3

Agentic AI risks

4

Proactive measures
for managing
Agentic AI risks

5

Key takeaways
and next steps



Agentic AI: Transforming industries by 2028

By 2028, leading firms predict widespread adoption of Agentic AI, with up to 80% of customer service automated, billions of AI agents in use, and significant impacts on enterprise decision-making and workflows.

Gartner By 2028

33% enterprise software will include Agentic AI

15% work decisions to be managed by Agentic AI

80% customer service issues to be autonomously resolved

40% enterprises will use AI to measure and influence employee behaviors

✓ **30%** cost reduction



By 2028

By 2026

1 billion

AI agents to be in service globally

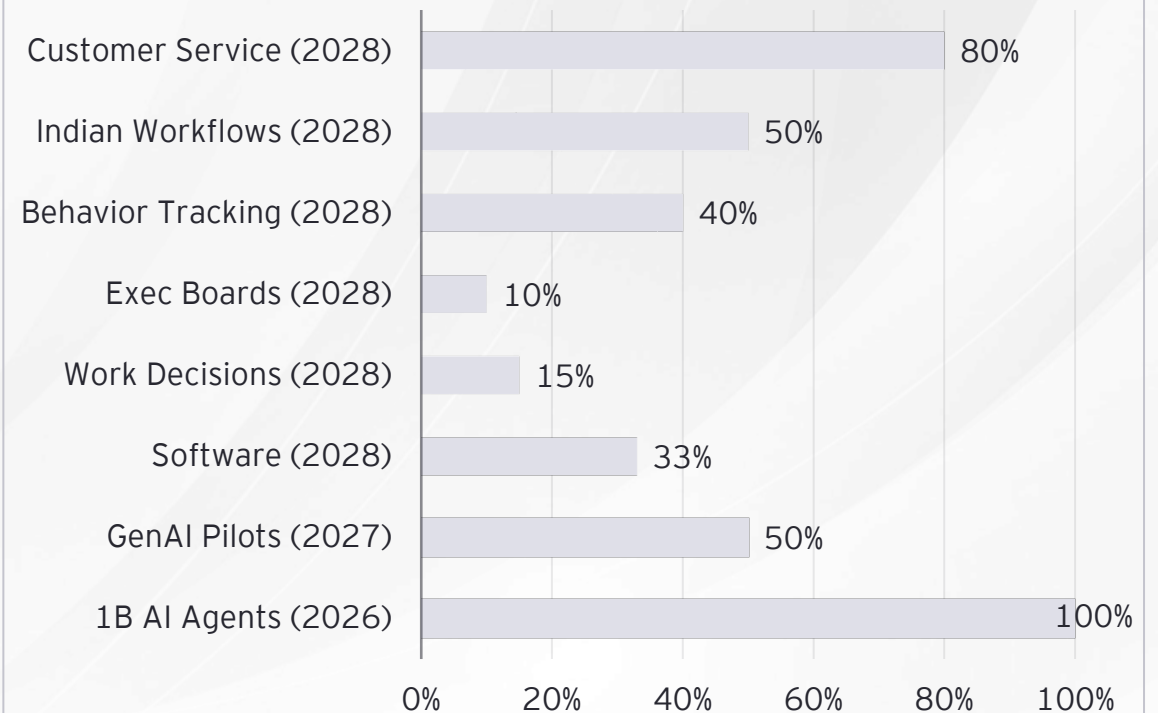
By 2028



AI will transform workflows

10% global boards to use AI guidance for executive decisions

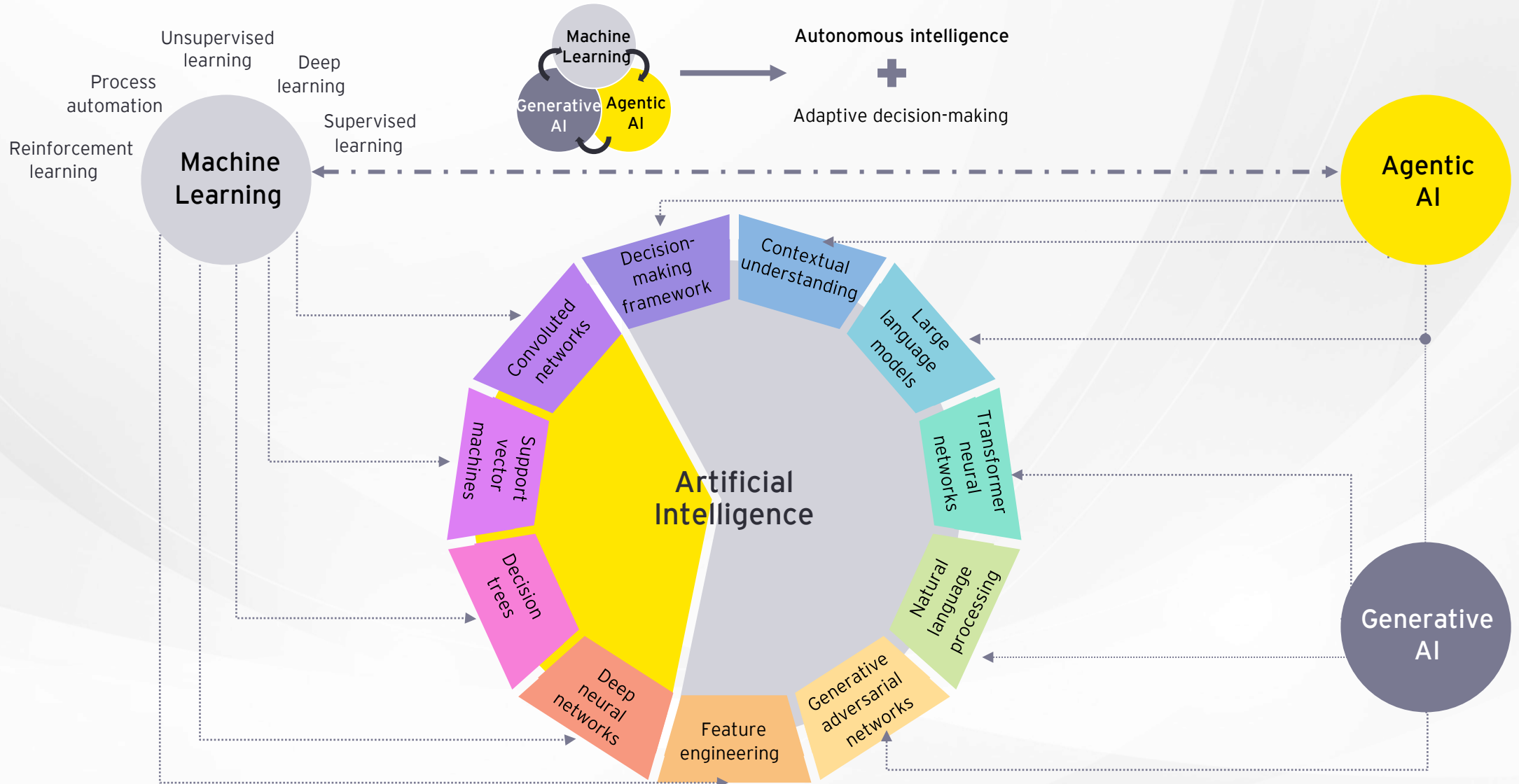
Statistical prediction about Agentic AI by 2028



Source : *Gartner, IBM*



Agentic AI: Bridging Generative AI and Machine Learning to enable autonomous intelligence and adaptive decision-making





What is Agentic AI?

What is Agentic AI ?

- Agentic AI is a form of artificial intelligence that enables autonomous decision-making, action, and continuous learning from interactions.
- It operates through autonomous AI agents that interpret context, make decisions, and execute actions aligned with preset objectives.

Agentic AI



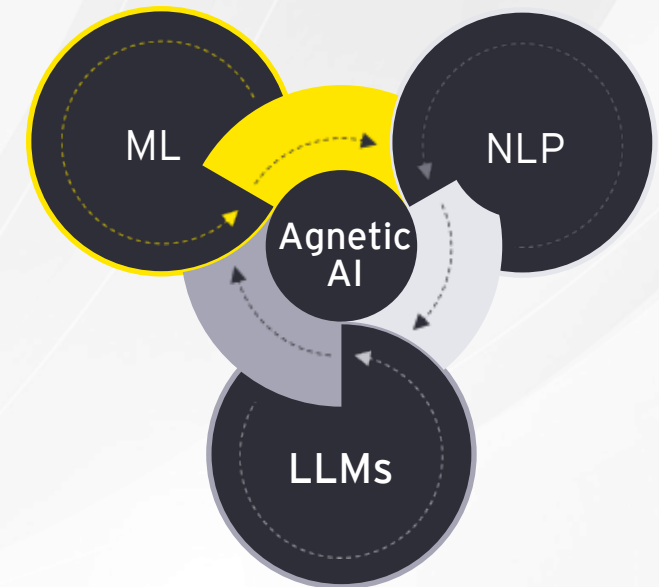
Autonomous

Ability to initiate and complete tasks independently, requiring minimal or no direct human supervision



Generative

Ability to continuously improve and adapt through interaction with its environment, learning from feedback

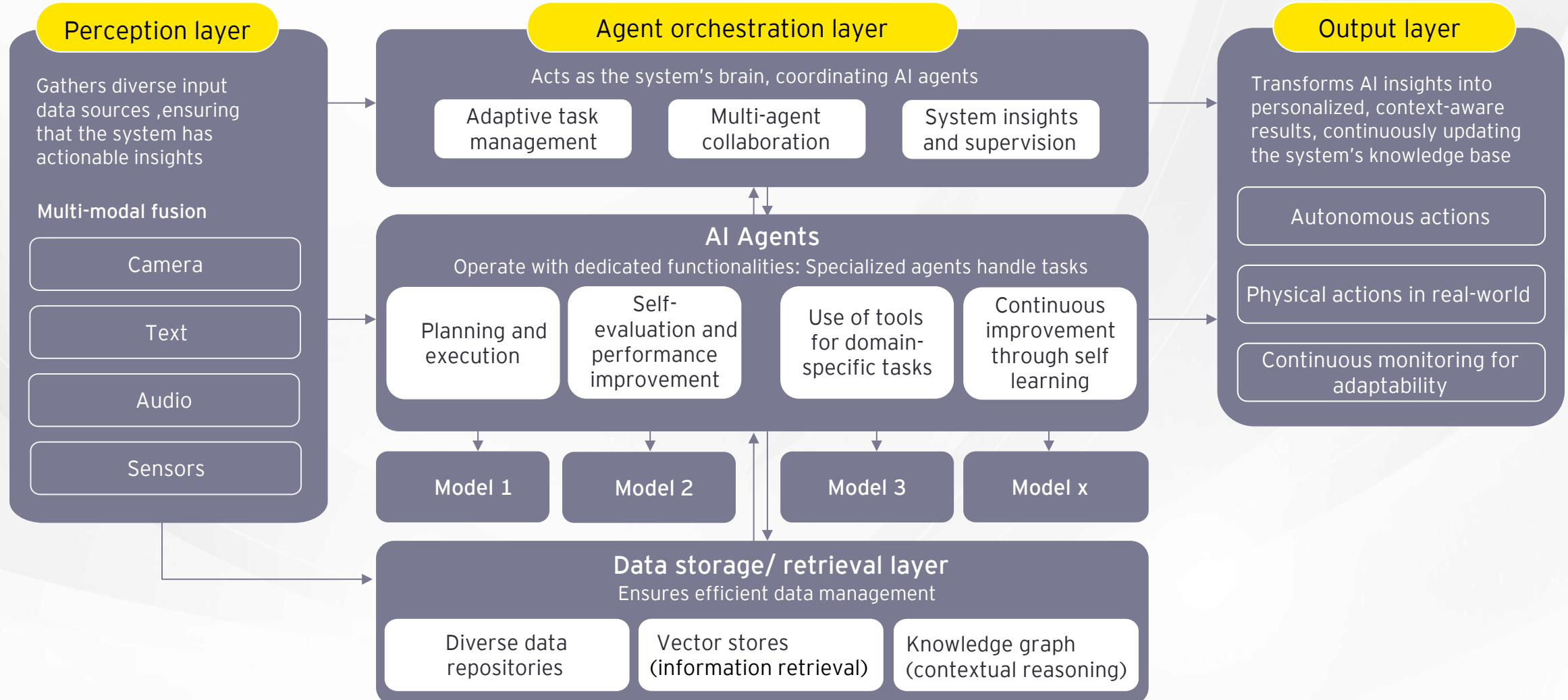


Combining these technologies with contextual understanding and decision-making frameworks results in a model that can:

- Handle complex, multi-step tasks with minimal oversight
- Generate text, media, and other outputs that are intuitive in communication with humans



Agentic AI architecture: A multi-layered framework enabling intelligent systems to perceive, orchestrate, and act autonomously with continuous learning and adaptability








Key features comparison: AI vs. Generative AI vs. Agentic AI




AI

Technology that enables machines to demonstrate human-like reasoning and capabilities.

-  Relies on structured/unstructured data for training and operation
-  Limited autonomy - it always needs human input or oversight
-  Complexity varies from simple rule-based systems to advanced learning algorithms

Generative AI

Subset of AI focused on creating new content, such as text, images, and code.

-  It needs vast data sets for training
-  Non-autonomous - output depends on user prompts
-  Advanced complexity - it needs deep learning architectures for training

Agentic AI

AI systems capable of autonomous decision-making and actions

- Uses real-time and historical data, including data it has generated itself, for context-aware decision-making
- Autonomous - capable of initiating actions without human prompts
- Highly complex - integrating AI decision-making with executions



Agentic AI adoption

Leading companies are leveraging Agentic AI to streamline operations and enhance user experiences. Examples include Google's workflow management platform, Saks' personalized shopping, OpenAI's browsing agent, Microsoft's chatbot, Amazon's conversational Alexa+, and Walmart's inventory optimization.

Google

Google has introduced an Agentic AI platform for enterprise workflow management

Saks

Saks, an American luxury retailer, is utilizing Agent AI to customize user shopping experiences

Open AI

OpenAI has launched Operator, an agent that can perform autonomous browsing

Microsoft

Microsoft has launched an Agentic chatbot to enhance customer engagement

Amazon

Amazon has unveiled an agentic Alexa+ that is more conversational

Walmart

Walmart is leveraging Agentic AI to optimize inventory management



Agentic AI potential across industries

Driving predictive insights, automation, and tailored solutions to enable the adoption of Agentic AI in healthcare, finance, manufacturing, transportation, and other sectors

Healthcare



Enhanced diagnostics

- Medical image analysis
- Improved accuracy



Personalized treatment

- Tailors plans to genetics and history



Streamlined administration

- Task automation and resource optimization



Predictive healthcare

- Proactive care for at risk individuals

Financial services



Autonomous decision

- Triggers trades
- Adjusts risk models



Efficiency gains

- Reduces manual workloads



Enhanced customer experience

- Automates financial management tasks

Manufacturing



Predictive maintenance

- Early failure detection
- Reduce downtime



Quality control

- Computer vision aided defect identification



Supply chain optimization

- Predicts demand
- Optimizes logistics

FMCG



Demand forecasting and inventory optimization

- Reduced waste and stockouts
- Smart production planning



Enhanced customer experience and personalization

- Targeted marketing campaigns
- 24/7 virtual assistance - AI-driven chatbots



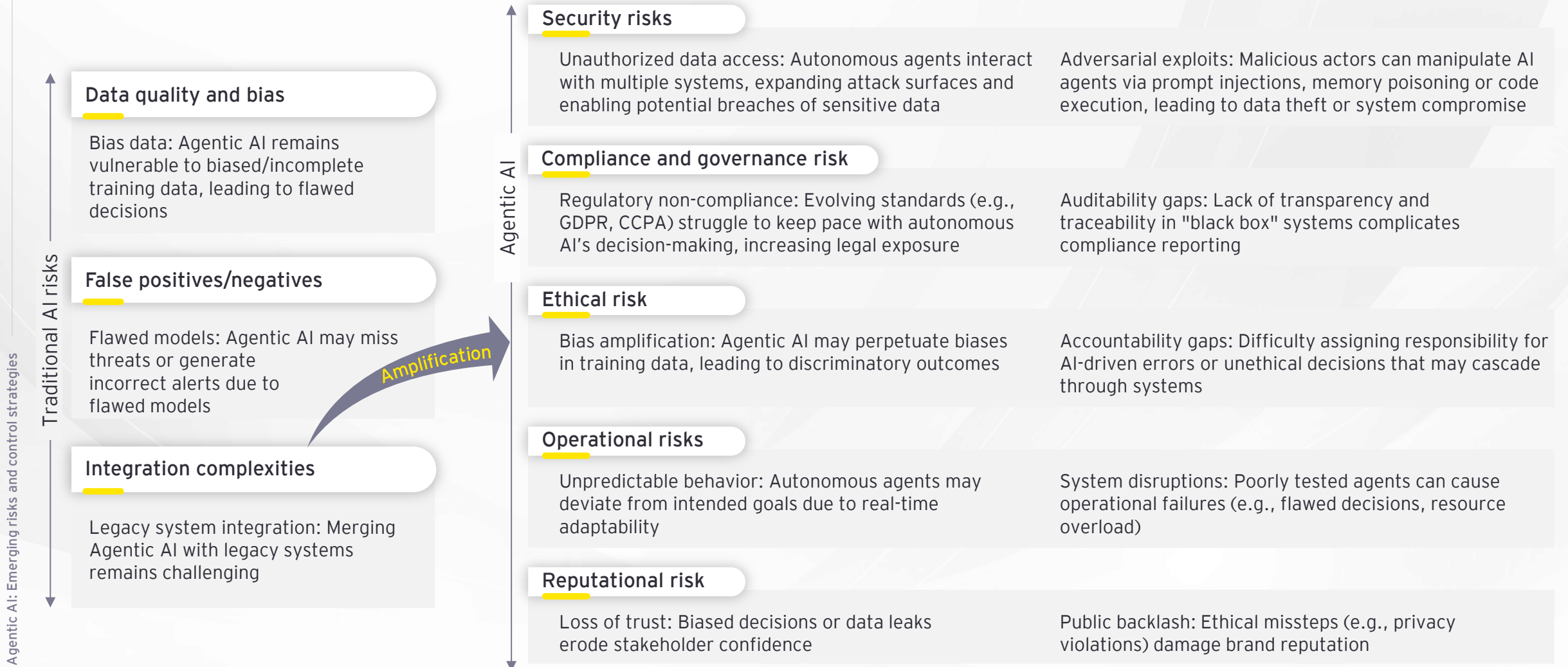
Product Innovation and quality control

- Consumer insights analysis
- Real-time quality monitoring





Agentic AI introduces amplified risks compared to traditional AI





Comprehensive risk mitigation: Safeguarding AI systems through security measures, transparency, ethical governance, fail-safe mechanisms, and compliance frameworks

Data privacy and compliance

Ensure compliance

Compliance with regulations like GDPR and CCPA

Regulatory alignment

Policies to align with frameworks like NIST AI RMF and ISO/IEC standards

Accountability structures

AI governance teams

- Establish cross-functional teams
- Define clear responsibility for AI outcomes to specific teams / individuals

Incidence response plans

- Define protocols for addressing breaches, biases, or system failures

Fail-safe mechanisms

Kill switch

Halt operations during malfunctions or attacks

Multi agent consensus verification

Reduce risks of rogue behavior

Continuous monitoring

SIEM tools to detect anomalies in real time



Source: [Reference Link1](#), [Reference Link2](#), [Reference Link3](#)

Security measures

Access controls

Implement RBAC/ABAC to limit agent privileges to minimal required tasks

Secure tool execution

Validate AI actions, enforce multi-factor authentication (MFA), and monitor command chaining

Transparency and explainability

Explainable AI (XAI)

Deploy interpretable models to audit decision logic

Immutable logs

Track all AI actions for accountability and compliance reporting

Ethical Guidelines & Governance

Bias Mitigation

Audit training data for fairness and enforce ethical guidelines

Human in the loop

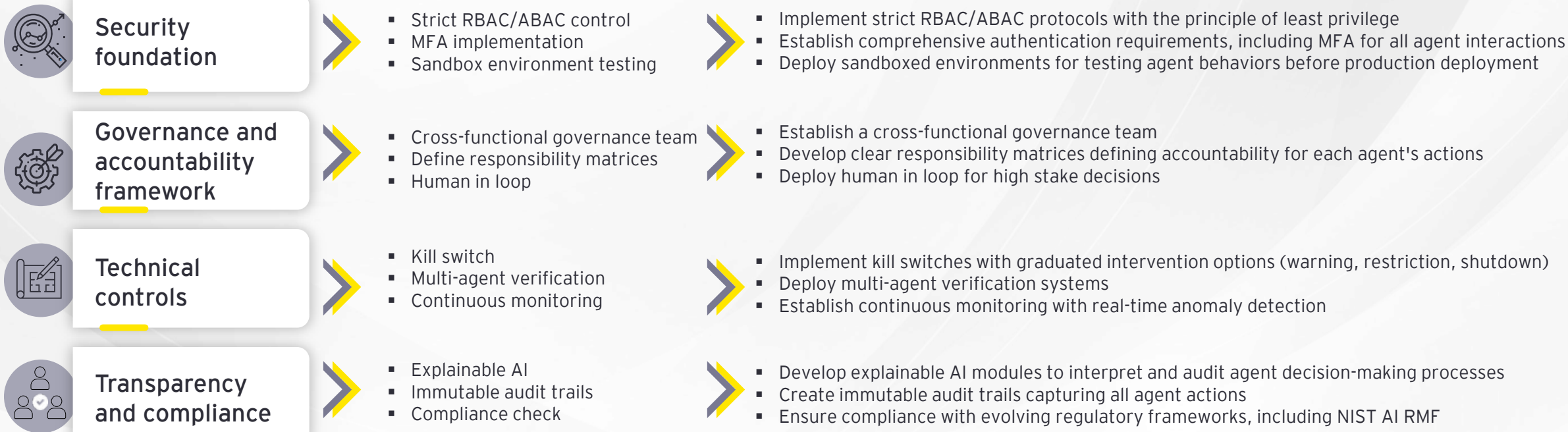
Require human approval for high-stakes decisions (e.g., healthcare diagnostics)



Key takeaways and the next steps

Agentic AI is a game-changer, offering unparalleled autonomy, efficiency, and innovation. While its risks—such as security vulnerabilities, accountability concerns, technical challenges, and transparency issues—are significant, they are manageable with the right mitigation strategies.

Implementation roadmap for the organizations



Our Offices

Ahmedabad

22nd Floor, B Wing, Privilon
Ambli BRT Road, Behind Iskcon Temple
Off SG Highway, Ahmedabad - 380 059
Tel: + 91 79 6608 3800

8th Floor, Building No. 14A
Block 14, Zone 1
Brigade International Financial Centre
GIFT City SEZ
Gandhinagar - 382 355, Gujarat
Tel + 91 79 6608 3800

Bengaluru

12th & 13th Floor
"UB City", Canberra Block
No.24 Vittal Mallya Road
Bengaluru - 560 001
Tel: + 91 80 6727 5000

Ground & 1st Floor
11, 'A' wing
Divyasree Chambers
Langford Town
Bengaluru - 560 025
Tel: + 91 80 6727 5000

3rd & 4th Floor
MARKSQUARE
#61, St. Mark's Road
Shantala Nagar
Bengaluru - 560 001
Tel: + 91 80 6727 5000

1st & 8th Floor, Tower A
Prestige Shantiniketan
Mahadevapura Post
Whitefield, Bengaluru - 560 048
Tel: + 91 80 6727 5000

Bhubaneswar

8th Floor, O-Hub, Tower A
Chandaka SEZ, Bhubaneswar
Odisha - 751024
Tel: + 91 674 274 4490

Chandigarh

Elante offices, Unit No. B-613 & 614
6th Floor, Plot No- 178-178A
Industrial & Business Park, Phase-I
Chandigarh - 160 002
Tel: + 91 172 6717800

Chennai

6th & 7th Floor, A Block,
Tidel Park, No.4, Rajiv Gandhi Salai
Taramani, Chennai - 600 113
Tel: + 91 44 6654 8100

Delhi NCR

Aikyam
Ground Floor
67, Institutional Area
Sector 44, Gurugram - 122 003
Haryana
Tel: + 91 124 443 4000

3rd & 6th Floor, Worldmark-1
IGI Airport Hospitality District
Aerocity, New Delhi - 110 037
Tel: + 91 11 4731 8000

4th & 5th Floor, Plot No 2B
Tower 2, Sector 126
Gautam Budh Nagar, U.P.
Noida - 201 304
Tel: + 91 120 671 7000

Hyderabad

THE SKYVIEW 10
18th Floor, "SOUTH LOBBY"
Survey No 83/1, Raidurgam
Hyderabad - 500 032
Tel: + 91 40 6736 2000

Jaipur

9th floor, Jewel of India
Horizon Tower, JLN Marg
Opp Jaipur Stock Exchange
Jaipur, Rajasthan - 302018

Kochi

9th Floor, ABAD Nucleus
NH-49, Maradu PO
Kochi - 682 304
Tel: + 91 484 433 4000

Kolkata

22 Camac Street
3rd Floor, Block 'C'
Kolkata - 700 016
Tel: + 91 33 6615 3400

6th floor, Sector V,
Building Omega, Bengal Intelligent
Park, Salt Lake Electronics
Complex, Bidhan Nagar
Kolkata - 700 091
Tel: + 91 33 6615 3400

Mumbai

14th Floor, The Ruby
29 Senapati Bapat Marg
Dadar (W), Mumbai - 400 028
Tel: + 91 22 6192 0000

5th Floor, Block B-2
Nirlon Knowledge Park
Off. Western Express Highway
Goregaon (E)
Mumbai - 400 063
Tel: + 91 22 6192 0000

3rd Floor, Unit No.301
Building No.1, Mindspace-Gigaplex
IT Park, MIDC, Plot No. IT-5
Airoli Knowledge Park
Airoli West, Navi Mumbai - 400 708
Tel: + 91 22 6192 0003

18th Floor, Altimus
Pandurang Budhkar Marg
Worli, Mumbai - 400 018
Tel: + 91 22 6192 0503

Pune

C-401, 4th Floor
Panchshil Tech Park, Yerwada
(Near Don Bosco School)
Pune - 411 006
Tel: + 91 20 4912 6000

10th Floor, Smartworks
M-Agile, Pan Card Club Road
Baner, Pune - 411 045
Tel: + 91 20 4912 6800

Ernst & Young LLP

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EYG member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/en_in.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at Ground Floor, Plot No. 67, Institutional Area, Sector - 44, Gurugram - 122 003, Haryana, India.

EYIN2506-001

© 2025 Ernst & Young LLP. Published in India.
All Rights Reserved.

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

ey.com/en_in



@EY_India



EY



EY India



EY Careers India



@ey_indiacareers