



REVA Academy for
Corporate Excellence



REVA
UNIVERSITY
Bengaluru, India

REVA UNIVERSITY PRESENTS

RACE

Technology Outlook

2026-27

Signals, Shifts and Strategic Bets
for the Enterprise

Released at RACEx360 2026

25 September 2026 · Taj West End, Bengaluru



RACEx360
Emerging Technology Conference 2026

An Annual Technology Leadership Publication From RACE, REVA University



Your Business is Moving. Is Your Technology Keeping Up?

Terralogic builds, modernizes, secures, and scales enterprise technology across legacy upgrades and AI implementations.

WHAT WE DO



AI & Data

Turn data into intelligence and action.



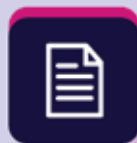
Application Development

Build, modernize, and manage business-critical applications.



Cybersecurity

Protect identities, data, systems, and operations.



Document Intelligence

Turn documents into searchable, usable business information.



IT & Managed Services

Keep your technology running, supported, and optimized.

**One technology partner.
Built for what's next.**

MODERNIZE → CONNECT → AUTOMATE → SECURE → SCALE

See What We Can Build Together



Leadership message

Building the future together

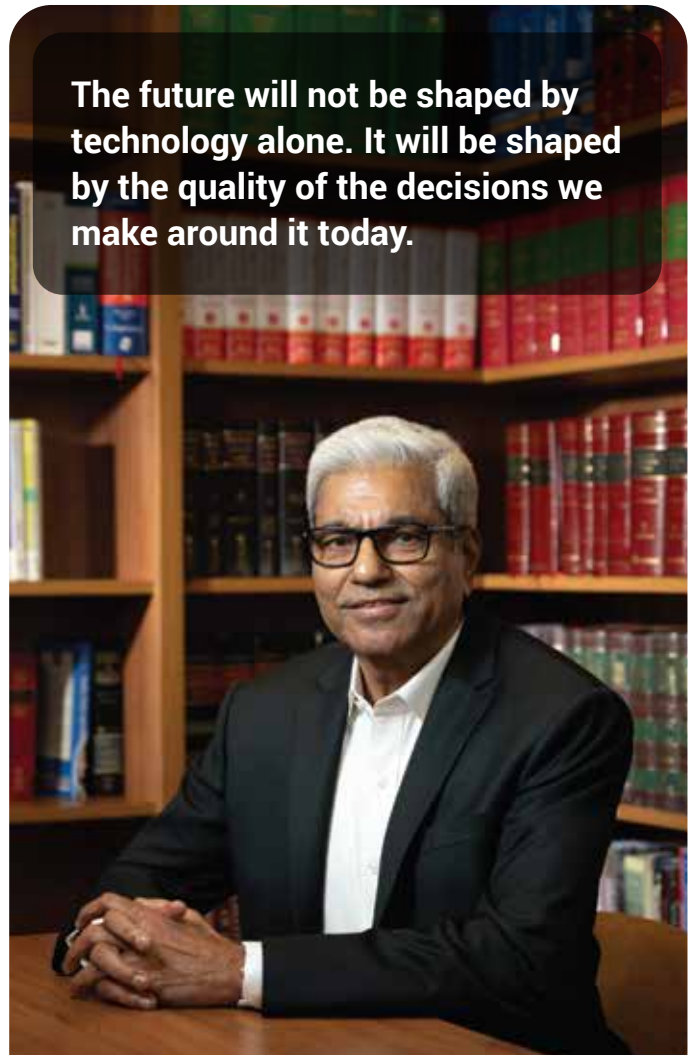
Technology is advancing at a pace that challenges every institution to think beyond the immediate. Artificial Intelligence, Cybersecurity, Cloud, Quantum technologies and intelligent physical systems are no longer separate conversations. Together, they are reshaping how organisations compete, how people work and how societies create value.

At REVA University, we believe that a university must do more than respond to these changes. It must create the conditions in which industry, academia and practitioners can examine them together, test ideas responsibly and translate emerging technologies into meaningful outcomes. REVA Academy for Corporate Excellence, RACE has built its work around this principle by bringing experienced professionals, enterprise leaders and applied research into the same learning and innovation ecosystem.

The RACE Technology Outlook 2026-27 is an extension of that commitment. It is not intended to predict technology for its own sake. It asks a more important question: what should leaders prepare for now? The perspectives in this edition examine the choices that will matter to enterprises over the next 12 to 24 months - from the economics of AI and the governance of autonomous systems to cyber resilience, post-quantum readiness, privacy and the changing nature of technology talent.

As India strengthens its position as a global technology and innovation hub, leadership will depend on our ability to combine ambition with responsibility, speed with judgement and innovation with trust. I hope this Outlook encourages informed debate, confident experimentation and stronger collaboration between industry and academia.

The future will not be shaped by technology alone. It will be shaped by the quality of the decisions we make around it today.



Dr. P. Shyama Raju
Chancellor, REVA University



Editor's note

Advantage is an operating capability

The most important technology question for a CXO in 2026 is no longer, 'Which technology should we adopt next?' It is, 'Can our organisation repeatedly turn fast-moving technologies into business advantage without losing control of cost, risk or optionality?'

That distinction matters. AI, cyber resilience, cloud, data, privacy, governance and talent are often managed as separate programmes, owned by different teams and measured by different scorecards. Yet the enterprise experiences them as one operating system. An AI agent is only as useful as the data it can trust, the permissions it is given, the cloud economics that sustain it, the controls that govern it and the people capable of supervising its decisions. Competitive advantage increasingly comes from connecting these capabilities, not from buying any one of them.



Dr. Shinu Abhi
Director, Corporate Training, RACE, REVA University

This is why the RACE Technology Outlook is organised around signals, strategic bets and decisions. We are deliberately less interested in declaring a technology 'hot' than in asking where it sits on the enterprise readiness curve, what it changes in the operating model and what leaders should do in the next 90 days. The goal is to preserve optionality: learn early, experiment frugally, own the critical architecture and commit capital only when evidence supports scale.

The seven outlooks in this edition reflect that operating logic. Frugal AI challenges the assumption that intelligence must always be expensive. Agentic AI shifts the discussion from assistance to delegated action. Post-quantum cybersecurity turns a distant scientific milestone into a present-day data-risk question. AI governance, privacy engineering and AI readiness move trust, value and accountability into the operating model itself. And the changing half-life of expertise reminds us that no technology strategy survives without a talent model that can keep learning.

Use the RACE Enterprise Technology Radar to challenge your portfolio. Use the CXO Technology Portfolio to decide what to scale, pilot, build capability around or simply watch. Use the checklists at the end of each article to move discussion from the conference hall to the next leadership meeting.

Technology advantage is not a collection of tools. It is an organisational capability - to sense earlier, decide better, learn faster and scale what works. That is the capability this Outlook is designed to strengthen.



Contents

Inside this edition

1 THE RACE SIGNAL

RACEx360 | Enterprise Technology Radar
| 7 Bets | CXO Technology Portfolio

2 SEVEN TECHNOLOGY OUTLOOKS

Frugal AI | Agentic AI | Post-Quantum
Cybersecurity | AI/GRC | Privacy | Talent
| AI Readiness & ROI

3 THE CXO AGENDA

10 questions every CXO should ask
before 2027

4 RACE ALUMNI IN ACTION

10 alumni stories in enterprise
leadership

5 THE RACE ECOSYSTEM

Learn | Build | Solve | Research |
Connect

6 PARTNERS & CONTRIBUTORS

Sponsor recognition | People
behind the Outlook



The convening

RACEx360 at a glance



RACEx360

Emerging Technology Conference 2026

25 September 2026 | Taj West End, Bengaluru

Why this convening

RACEx360 brings enterprise leaders, technology decision-makers, practitioners and innovators into one day of high-intensity conversation, demonstration and curated engagement, followed by the Top 10 Women Tech Leaders India Awards 2026 & Gala Dinner.

650+
Delegates

150+
CXOs & senior leaders

60+
Speakers

Four conference themes

1. GenAI and Agentic AI
2. Cloud and Platform Engineering
3. Cybersecurity in the AI era
4. Deep Tech and Sustainability

Evening

Top 10 Women Tech Leaders India Awards 2026

4th Edition | Awards and Gala Dinner



RACEx360 2026

Programme & Keynote Snapshot

Main Stage + Hall B Experiences + Curated CXO Engagements

Taj West End Court - Hall A – Ideas that shape the future

TIME	TITLE	SPEAKERS
8:30–9:15	Delegate Registration & Seating	—
9:30–10:15	RACEx360 2026 Opening Ceremony	Welcome & Conference Brief Presidential Address: Dr. P. Shyama Raju, <i>Chancellor, REVA University</i>
10:15–10:20	Official RACE360 Technology Outlook Book Release	All Dignitaries
10:20–10:50	Building India's AI-Native Enterprise: From Generative AI to Autonomous Intelligence	National Keynote Mathangi Sri Ramachandran, <i>CoFounder YuVerse</i>
10:50–11:10	Building the Autonomous Enterprise: From AI Adoption to Secure, Scalable Intelligence	Vision Address I Renil Komitla, <i>Founder & CEO, Terralogic</i>
11:10–11:30	Building Before the Curve: From NFC Payments to the Post-Quantum Enterprise	Vision Address II: Jorge Fernandes, <i>Chairman, CEO & Co-Founder, iBlades.ai</i>
12:00–12:45	Panel 1 - GenAI & Agentic AI: Beyond the Chatbot: Building AI Agents That Deliver Business Outcomes	Moderator: Soumik Ghosh (The Economic Times) Panellists: Jagannath P. V. (LTIMindtree) Shaista Lodi (Philips) Smitha Mave (Google) Pradeepta Mishra (Beghou) Suvarcha Arora (FIS) Kunal Ruvala (Palo Alto Networks)
14:00–14:05	Digital Forensics Playbook	Book Launch Nishant Krishna, <i>Executive Director, Visiminds</i>
14:05–14:50	Panel 2 - Cloud & Platform Engineering: The AI-Native Cloud: Platforms for Agents, GPUs and Always-On Intelligence	Moderator: Vaishnavi Desai (The Economic Times) Panellists: Sajan Liyon (Broadcom / VMware) Sudarshan Balakrishna (Epsilon) Naresh Choudhary (Infosys) Punit Santani (Capgemini) Channaveer B. Biradar (Syngene International)
14:55–15:25	Fireside Chat DeepTech: Beyond AI: Quantum, Space & the Next Security Frontier	Moderator: Rajiv Chetwani (ISRO) · Krishna Pandey (PropertyGuru Group) · Dr. Vishal Saraswat (Bosch)



RACEx360 2026

Programme & Keynote Snapshot

Main Stage + Hall B Experiences + Curated CXO Engagements

Taj West End Court - Hall A – Ideas that shape the future

TIME	TITLE	SPEAKERS
15:30–16:15	Panel 3 - Cybersecurity in the AI Era: AI versus AI: Defending the Autonomous Enterprise	<i>Moderator:</i> Soumik Ghosh (The Economic Times) Dr. Vishal Saraswat (Bosch) Shashank Bajpai (Yotta Data Services) Lakshminarayanan R. S. (Wipro) Deepa Seshadri (Deloitte India) Surendra Nemani (Hexaware)
16:35–17:05	Fireside Chat Sustainability Beyond Compliance: Building the Intelligent, Low-Carbon Enterprise	<i>Moderator:</i> Shreya Krishnan (AnitaB.org) Shrutee Ganguly (Turner & Townsend) Suba Lakshminarasimhan (Executive Alchemy 365)
17:10–17:30	From Boardroom to Bharat: Delivering AI at Population Scale	Closing Keynote: Gautham Krishnamurthy, <i>Head of Product, Consumer Platform, PhonePe</i>
17:30–17:45	Key Insights, Audience Pulse & What Next	Conference Synthesis: Dr. J. B. Simha, <i>Chief Mentor, AI, REVA University</i>
17:45–18:00	Audience Winner Announcements · Recognition of Partners, Organising Team & Volunteers	Day Conference Close: Dr. Shinu Abhi, <i>Director, Corporate Training, RACE, REVA University</i>

Top 10 Women Tech Leaders India Awards 2026: Hall A (6:30 PM onwards)

18:35–18:45	Opening of the Top 10 Women Tech Leaders India Awards 2026	All Dignitaries
18:45–18:55	Jury Remarks, Awards Unveiling & Coffee-Table Book Release	Deepa Seshadri (Deloitte India) Rama Kini (Terralogic Inc.) Latha Chembrakalam (AutoAscend) Dr. Ram Kumar G (Cybersecurity Leaders, Global Automotive) Sandeep Vijayaraghavan (Terralogic Inc.)
18:55–19:00	Presidential Remarks	Dr. P. Shyama Raju, <i>Chancellor, REVA University</i>
19:00–19:40	Presentation of the Top 10 Women Tech Leaders India Awards 2026	2026 Awardees
19:40–19:55	Felicitation of Past Award Winners	Past Winners, Women Tech Leaders India Awards
19:55–20:00	Vote of Thanks	Dr. Shinu Abhi, <i>RACE, REVA University</i>

Programme sequencing is subject to final production and speaker confirmations.



RACEx360 2026

Programme & Keynote Snapshot

Main Stage + Hall B Experiences + Curated CXO Engagements

Experience Zone: Grand Ball Room, Hall B (12:00 PM – 4:55 PM)

TIME	EXPERIENCE ZONE	SPEAKERS
12:00–12:30	Unified Security Solution: FlyView, Identity, Data, AI & Cloud Security	Sandeep V <i>EVP - Terralogic Inc.</i>
12:30–13:00	Live Enterprise Cyber Resilience: The NetTron Solution (GuardTron & ManoTron)	Jorge Fernandes & Ashok Kavichandran, <i>Founders, iBlades.ai</i>
14:10–14:30	Governing Agentic AI at Enterprise Scale: Docker AI Governance & Software Supply-Chain Security	Sundar Vedaraman, <i>Sr. Technical Account Manager, Docker</i>
14:30–14:50	Sovereign Cloud, AI Security: Cosol Cloud & Cosol AI Security	Kirankumar H B, <i>Head – Alliances & Technology, Cosol</i>
14:50–15:10	Unified Security across VMs & Containers: Nutanix Flow	Amit Gupta <i>Sr. Product Manager, Nutanix</i>
15:10–15:25	See Everything, Fear Nothing: NetWitness SOC Platform	Sanyum Sharma, <i>Senior SE India, NetWitness India</i>
15:25–15:40	Intelligence X Compounded: The Intelligence X Compound Suite	Vinay Tadimalla, <i>Director Technology TSMT</i> Srividya Athresh, <i>Head, CRM, TSML</i>
15:40–15:55	Code Scanning & Vulnerability Assessment: Visiminds Ivy (Ivy Lens & Ivy Insight)	Nishant Krishna <i>Executive Director, Visiminds</i>
15:55–16:10	Build Secure Software in an AI Era: CleanStart Hardened Container Images	Dhanush VM, <i>Solution Architect, CleanStart</i>
16:10–16:25	Astrikos AI Platform: SAP Platform, Industrial Intelligence	Ali Sadhik Shaik, <i>Chief Product Officer, Astrikos AI</i>
16:25–16:40	Non-Human Identities Are Taking Over Your Enterprise	Jothiram Selvam & Fizer Khan, <i>CEO & CTO, NamLabs Technologies</i>
16:40–16:55	Accelerating Enterprise AI with HPE Compute: HPE Compute + AI	Neha Khan, <i>Business Development Executive, Care Point</i>

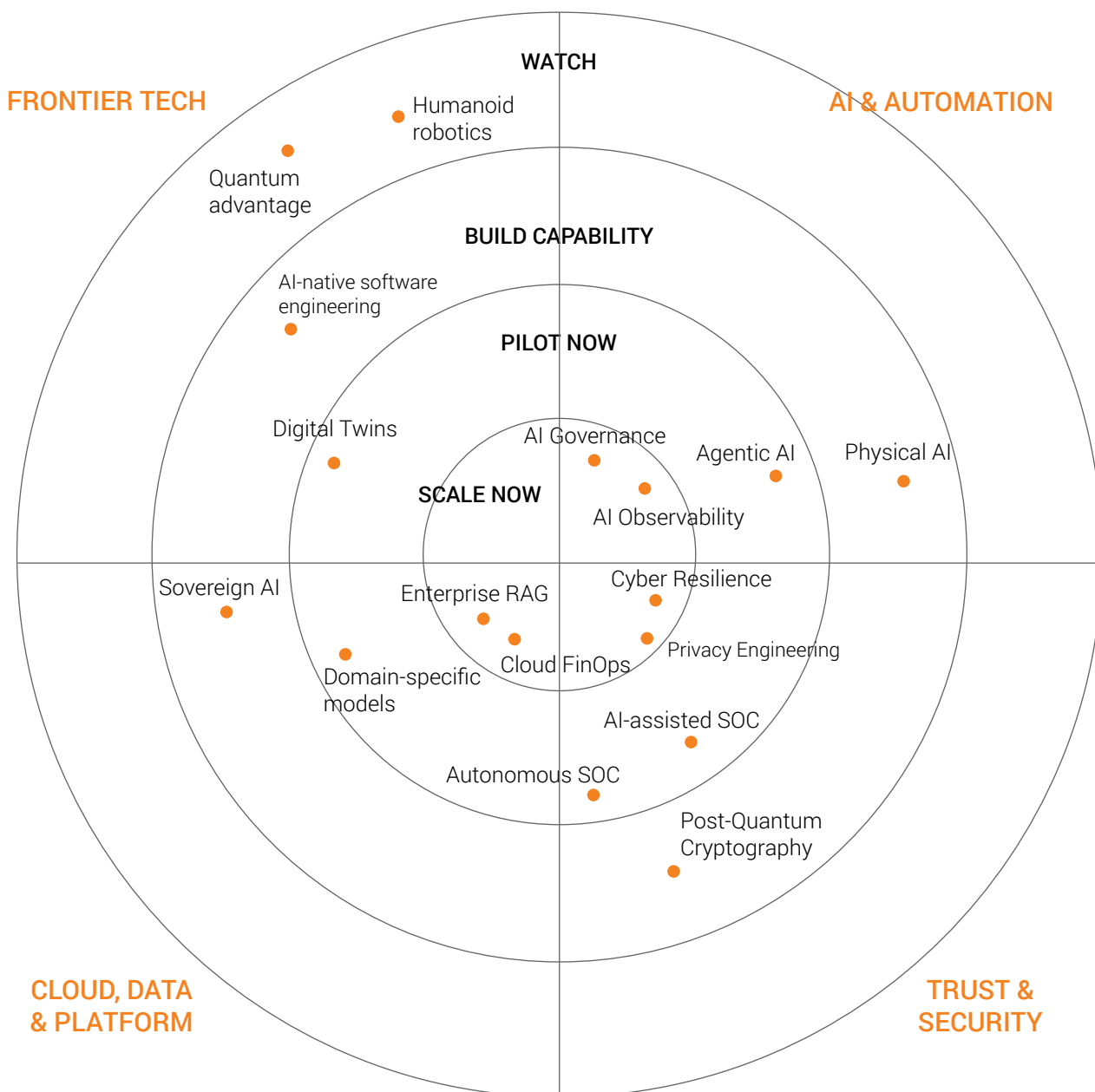
Programme sequencing is subject to final production and speaker confirmations.



The signature asset

RACE Enterprise Technology Radar 2026–27

A directional view of what to scale, pilot, build capability around and watch.



RACE editorial assessment. Positioning reflects enterprise readiness, likely business impact and adoption horizon - not a market forecast or investment recommendation.



Reading the radar

Readiness × impact × adoption horizon

Technology	Enterprise readiness	Potential impact	Adoption horizon
AI governance	High	High	Now
AI observability	High	High	Now
Cyber resilience	High	High	Now
Privacy engineering	High	High	Now
Cloud FinOps	High	Medium–High	Now
Enterprise RAG	High	High	Now
Agentic AI	Emerging	Very High	Next
AI-assisted / autonomous SOC	Emerging	High	Next
Small / domain-specific models	Emerging	High	Next
Physical AI	Emerging	High	Next
Digital twins	Emerging	Medium–High	Next
Post-quantum cryptography	Emerging	Very High	Build now
Sovereign AI	Emerging	High	Build now
AI-native software engineering	Emerging	High	Build now
Quantum advantage	Experimental	Very High	Watch

The purpose of the radar is not to declare winners. It is to force portfolio discipline: what deserves operating investment now, what deserves controlled experimentation, and what deserves awareness without premature commitment.



Authored by RACE

RACE's 7 enterprise technology bets for 2027

The most important shifts we expect enterprise leaders to manage over the next 12–18 months.

01



AI moves from copilots to accountable agents.

The governance question shifts from “what can the model say?” to “what can the agent decide and do?”

02



Smaller, specialised AI models challenge “bigger is better”.

Unit economics, privacy and latency make model portfolios more important than model prestige.

03



AI governance moves from policy to runtime control.

Autonomous systems force governance, model risk and continuous controls into the technology stack itself.

04



Crypto-agility moves onto the enterprise risk agenda.

PQC readiness starts with knowing where cryptography lives and being able to swap it.

05



Privacy evolves from compliance to architecture.

Consent, lineage, purpose and accountability must be engineered into data and AI systems.

06



AI ROI moves from pilots to operating readiness.

The winners will fund data, governance, workflow redesign and measurement - not just models.

07



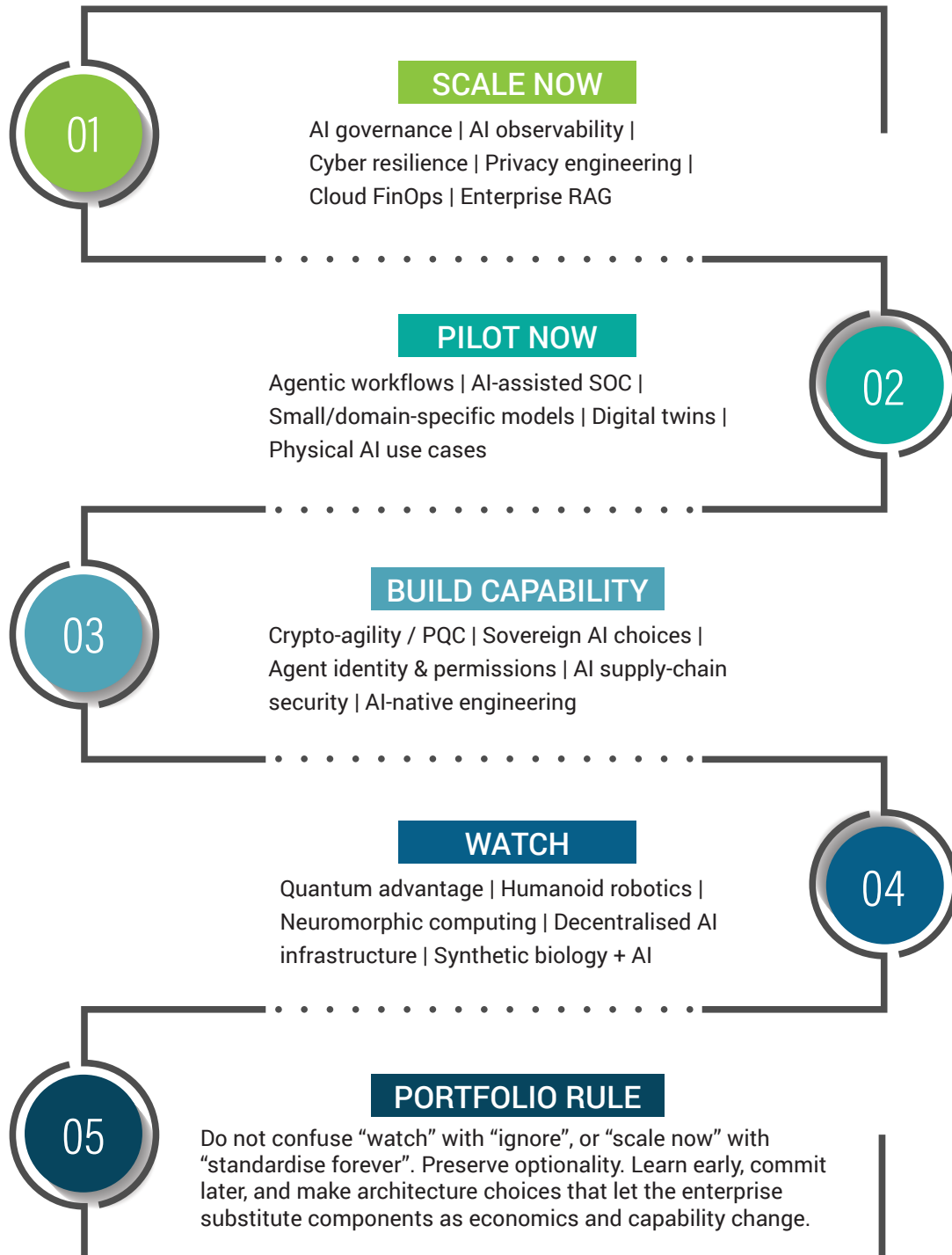
AI skills shift from tool proficiency to systems thinking.

Human judgement, orchestration and evidence of capability become more valuable than static credentials.



The 2027 CXO technology portfolio

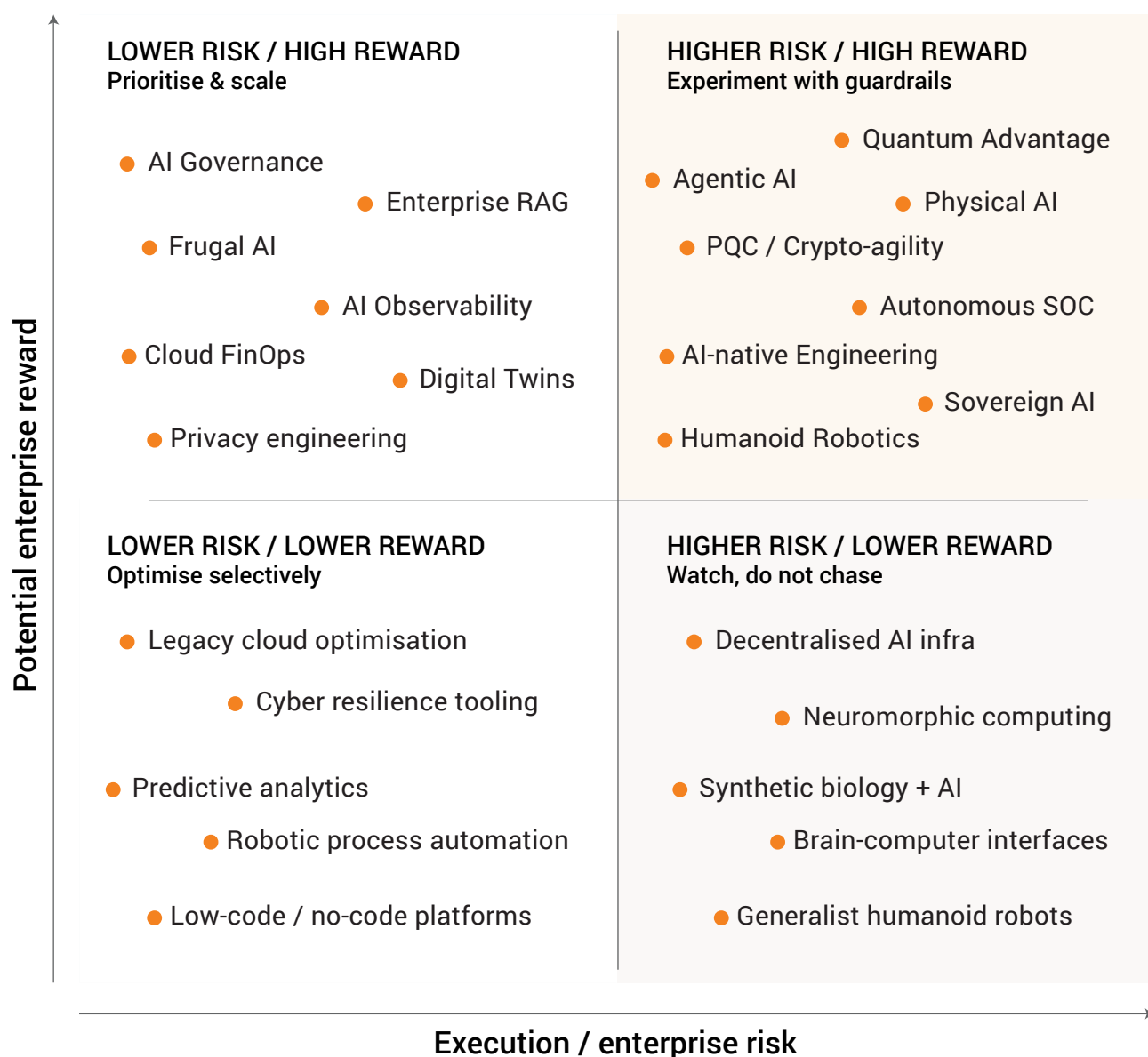
What to scale, pilot, build capability around and watch



Decision lens

Risk × reward for emerging enterprise technologies

A second view for deciding where experimentation deserves executive attention.



The upper-right quadrant is not a “do not invest” zone. It is where executive sponsorship, guardrails and staged experimentation matter most.



Section 01

Seven technology outlooks

Seven signals |
Seven enterprise decisions |
One operating capability



Section 01

01

Frugal AI

Less compute | More intelligence:
The rise of frugal AI

Dr. Jay B. Simha

CAIO, adoptAI Technologies | Chief AI Mentor, RACE



01 · Frugal AI

Less Compute | More Intelligence: The rise of frugal AI



By **Dr. Jay B. Simha** | CAIO, AdoptAI Technologies | Chief AI Mentor, RACE REVA University

Dr. Jay B. Simha is an AI and analytics technology leader with 20+ years of industry experience across telecom, BFSI, manufacturing, and enterprise applications. A Ph.D. in AI, he has led AI/ML innovations in predictive analytics, deep learning, and decision support. His current research and consulting focus on Frugal AI for enterprise.



FOCUS

Smaller models, efficiency, cost, edge AI and disciplined enterprise value.

01 | The Signal

AI is becoming dramatically more capable, but enterprise AI is also becoming progressively more expensive to build, operate and govern. The temptation is to respond with a big-bang programme: pick a powerful foundation model, connect every data source, deploy agents everywhere and let adoption follow. That approach can create impressive demonstrations while quietly increasing cost, dependency and organisational complexity.

The alternative is Frugal AI: achieving the required business outcome with the least

necessary combination of models, data, compute, integration and human effort. Frugality is not about choosing the cheapest model. It is about engineering for value.

For enterprises, this means asking a different question. Instead of 'Where can we use AI?', ask 'Where does AI create measurable advantage, and what is the smallest reliable AI system that can deliver it?' The goal is not to resist powerful AI, but to deploy intelligence selectively, where it earns its place through measurable business value.

02 | Why now

The enterprise AI landscape has matured quickly. There are now many capable foundation models, open and proprietary, alongside rapidly evolving agentic frameworks. Their capabilities increasingly overlap, but their economics, reliability, privacy characteristics, latency and governance requirements differ.

This creates a strategic choice for CIOs and business leaders. Building everything around one external model may be fast at first, but it

can create vendor dependency and make economics hard to control as usage scales. Running a large model everywhere can be unnecessary when a smaller model, a retrieval system, a rules engine or a conventional analytics model can solve the task well enough.

Frugal AI therefore starts with ownership of the decision architecture, not necessarily ownership of every model. Enterprises should know which tasks need frontier intelligence,



which can be handled by smaller specialised models, where retrieval and enterprise knowledge add value, and where deterministic software is safer. The principle is simple: own the architecture, tune the components,

measure the outcome. Trust matters just as much. An AI system that is cheap but unreliable is not frugal; it simply moves cost from the technology budget to operational risk.

03 | Enterprise impact

The impact of Frugal AI will be felt first in cost, risk and the operating model. Consider an enterprise customer-service operation handling thousands of interactions a day. A frontier model could be used for every interaction, but that may be economically unnecessary.

A frugal architecture could classify incoming requests with a small model, retrieve approved enterprise knowledge, use deterministic workflows for routine transactions, and call a larger model only when the case needs complex reasoning. Human agents stay in the loop for high-risk or ambiguous cases. The result is not just a lower inference bill. It can cut latency,

improve consistency, limit data exposure and make the system easier to audit.

The operating model also changes. AI teams move from being model consumers to AI system engineers. Their job becomes selecting, evaluating, tuning and governing a portfolio of models and components against business outcomes. Talent benefits from this shift: organisations need people who understand business processes, data quality, evaluation, security and cost alongside AI capabilities. Most importantly, Frugal AI makes scaling more disciplined, turning AI from an experimentation budget into an engineered enterprise capability.

04 | What CXOs should do

1. Start with economics, not models. Define the business outcome, acceptable error rate, latency requirement and maximum cost per transaction before selecting technology.
2. Build a model portfolio. Use frontier models where they create differentiated value and smaller, specialised or open models for simpler workloads.
3. Establish an AI evaluation layer. Measure accuracy, groundedness, safety, latency and cost continuously.
4. Own the enterprise knowledge and control plane. Keep curated data, retrieval, policies, prompts, evaluation datasets, workflow logic and observability under enterprise control.
5. Scale by evidence. Move from pilot to production only when a use case shows measurable business value, acceptable risk and sustainable unit economics.



05 | The 2027 prediction

By 2027, leading enterprises will measure AI success less by the size or sophistication of the model they deploy and more by AI unit economics: business value delivered per rupee, per second of latency and per unit of compute. Frugal AI will become an enterprise architecture principle, not just a cost-saving tactic.

"Make your AI: own it, tune it."

The CXO checklist

Three questions for your leadership team

1. Do we have what a frugal AI use case needs: a clear use case, the data, the subject-matter expertise and a baseline to compare against?
2. Does our organisation have an evidence-driven culture?
3. Do we have the budget and the mindset to adopt AI?

One move to make in the next 90 days

Run a PoC or PoV on a low-hanging use case with frugal AI, and compare it against using the latest foundation model.



SECURITY SOFTWARE AND SERVICES

Security for what you build, and for what you run.



Code and app security. Your code, its packages, secrets and mobile builds, checked on your own machine. Nothing goes to a cloud.



The systems you run. Hosts, web applications, APIs and cloud accounts, checked as often as you like, from inside your network.

WHERE VISIMINDS CAN HELP

VCISO consulting

Security leadership for your organisation, on demand

GRC

Governance, risk and compliance, with the evidence to show

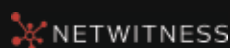
VAPT

Vulnerability assessment and penetration testing

Cyber forensics

Investigation, evidence and what to change after

Ivy Lens and Ivy Insight are Visiminds Technologies products
Walkthrough on request: info@visiminds.com

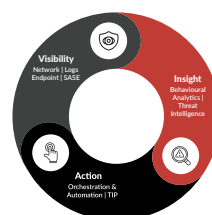


NetWitness Platform Defense Accelerated

DATASHEET

NetWitness® Platform delivers the most complete toolset for threat detection, investigation, response, and forensics. Featuring unmatched visibility, deep analytics, and robust response actions, NetWitness supports the requirements of the most security-conscious organizations around the globe.

Use Case	Customer Issues	How Does NetWitness Address Issues?
Threat Detection and Response	Detecting attacks and exploits that evade perimeter defenses	• Obtain visibility into an organization's IT infrastructure, across cloud, on-premises, and hybrid architectures • Apply advanced analytics and threat intelligence to identify indicators of compromise (IoCs) that warrant investigation • Provide advanced tooling to analyze and investigate anomalies, and remediate them
Incident Forensics	Reveal the full scope of an attack	• Correlate events that comprise an attack, wherever they happen across an organization's IT infrastructure • "Replay" the attack through network packets to understand the process used by the attackers • Create a report for Board and Regulatory staffs to document the attack and prevent future ones
User Entity and Behavior Analytics (UEBA)	Detecting anomalous or risky behaviors	• Create a baseline for "normal" activity by people and IT systems • Flag behaviors that deviate from the normal ones and adjust baseline as normal behaviors evolve • Create reports for compliance and documentation



Visibility

NetWitness Platform delivers unrivaled visibility into your organization's data by collecting and analyzing logs, packets, endpoint, NetFlow, and IoT/OT data across all computing platforms, including physical, virtual, cloud, and hybrid deployments.

Insight

NetWitness applies advanced analytics and threat intelligence to detect and correlate attacks so you can stop them before they damage your operations and reputation.

Action

NetWitness makes detections actionable with tools that block processes, isolate infected applications and endpoints, and re-image hardware.



Section 01

02

Agentic AI

From copilots to coworkers:
The agentic enterprise

Pradeepta Mishra
VP of AI, Beghou



02 · Agentic AI

From copilots to coworkers: The agentic enterprise



By **Pradeepta Mishra** | VP of AI, Beghou

Pradeepta Mishra is a senior AI leader, author, inventor, and educator with over two decades of experience in artificial intelligence, machine learning, and data science. He is VP of Artificial Intelligence at Beghou Consulting and a Consulting Magazine Top Consultant 2026, with 17 patents, 11 books, and extensive industry expertise.



FOCUS

Autonomous workflows, multi-agent systems, orchestration, governance and ROI.

01 | The Signal

Enterprise AI is moving from copilots that wait to be asked to agents that take a goal and run with it: planning across steps, calling tools, making decisions, and following a task through to completion. The unit of work is shifting from the prompt to the outcome. Where a copilot drafted an email for someone to send, an agent now reconciles the accounts, resolves the ticket, or closes a workflow end to end, looping in a human mainly at exceptions. This is not a bigger chatbot; it is a change in where humans sit relative to the work: from doing every step to setting the goal, defining the guardrails, and reviewing what gets escalated. The question for leadership is no longer which team gets a copilot, but which outcomes you are willing to delegate, and under what supervision.

02 | Why now

Three things converged. Models became reliable enough at multi-step reasoning and tool use to make acting, not just suggesting, a defensible bet for a growing set of tasks. Standardised ways for AI systems to connect to internal databases, CRMs, ticketing systems, and codebases matured, so an agent can reach the systems of record it actually needs rather than just talking about them. And several years of building evaluation muscle around AI output gave enterprises the logging, review queues, and escalation paths required to supervise something more autonomous than a chat window. None of this makes agents ready to run unsupervised everywhere. It means the infrastructure now exists to deploy them carefully, in bounded domains, with humans at the checkpoints that matter, which is why 2026-27 is when this moves from pilot to production.

03 | Enterprise impact

The clearest impact so far is not in dramatic, fully autonomous transformation; it is in high-volume workflows with clear success criteria. In software engineering, agents now read an issue, write the code, run the tests, and open a pull request end to end, with a developer reviewing the diff rather than typing every line; teams report material cuts in cycle time on routine fixes. The same pattern is



spreading to customer support, where agents resolve routine tickets and escalate only what needs judgment, and to finance operations, where agents reconcile records across systems and draft exception reports for sign-off. The cost upside is real, but so is the risk shift: a bad co-pilot suggestion costs someone a few minutes to reject, while a bad agent action that has already executed can cost real money, a damaged customer relationship, or corrupted data. Talent needs are shifting too, fewer people producing first drafts, more people defining what "good" looks like, designing escalation logic, and owning outcomes they did not personally execute.

04 | What CXOs should do

1. Map your workflows on two axes; volume and reversibility; start agentic pilots where volume is high and mistakes are cheap to undo.
2. Redesign permissioning before deployment: decide exactly which systems, data, and actions an agent can touch, applying the same least-privilege discipline you would to a new hire.
3. Build checkpoints into the workflow, not just a review of the output. Define where a human must approve before anything irreversible goes out, such as a payment, a customer message, or a production change.
4. Invest in auditability now: require agents to log not just what they did but why, so failures can be traced and fixed rather than just reversed.
5. Reskill the people whose drafts get automated toward supervising, correcting, and being accountable for outcomes they did not personally execute. This is a new job, not a smaller version of the old one.

05 | The 2027 prediction

By late 2027, most large enterprises will have at least one production workflow run predominantly by an agent, with human review reserved for exceptions and the real differentiator won't be who adopted agents first, but whose guardrails actually held.

"The enterprises that win won't be the ones that deployed the most agents first, they'll be the ones that worked out exactly how much autonomy to grant, and built the checkpoints to make it trustworthy."

The CXO checklist

Three questions for your leadership team

1. Do we have what a frugal AI use case needs: a clear use case, the data, the subject-matter expertise and a baseline to compare against?
2. Does our organisation have an evidence-driven culture?
3. Do we have the budget and the mindset to adopt AI?

One move to make in the next 90 days

Pick one bounded, reversible workflow and run a supervised agent pilot with a hard human checkpoint before anything external ships.



Section 01

03

Post-quantum cybersecurity

Before Q-Day:
Why crypto-agility cannot wait

Sridhar Govardhan
Group CISO, Angel One

03 · Post-quantum cybersecurity

Before Q-Day: Why crypto-agility cannot wait



By **Sridhar Govardhan** | Group CISO, Angel One

Sridhar Govardhan is a seasoned technology and business leader with extensive experience across IT/ITES, e-commerce, Web3 and financial services. He has held leadership roles driving technology, information security, digital transformation and business resilience across fast-paced, technology-led organisations. At Angel One, he leads the organisation's cybersecurity and risk strategy, with a strong focus on enabling innovation, responsible AI adoption, customer trust and sustainable business growth.



FOCUS

PQC, cryptographic inventories, migration, long-lived data and enterprise readiness.

01 | The Signal

For the past three decades, the security of the internet's trust mechanism has rested on a single mathematical wager: that it will stay computationally infeasible to factor large prime numbers and to compute discrete logarithms. That wager is expiring fast. A sufficiently powerful quantum computer running Shor's algorithm can break RSA, Diffie-Hellman and elliptic-curve cryptography - the mathematical basis for virtually all TLS handshakes, code signatures and digital certificates - in minutes instead of centuries.

The forcing factor is not the day an adversary switches on a cryptographically relevant quantum computer. It is the day an adversary collects today's encrypted traffic, stores it, and decrypts it later. That second event, commonly referred to as Q-Day, makes retroactively vulnerable every record whose confidentiality must outlast the wait. The transition is no longer speculative. It has a blueprint.

02 | Why now

In 2026 and 2027, three factors are converging. First, regulatory requirements are rising and post-quantum migration deadlines are beginning to influence enterprise roadmaps. Second, most organisations have built up decades of largely invisible cryptographic debt: RSA, ECDSA and ageing algorithms embedded in authentication workflows, document-signing processes, software supply chains and hardware roots of trust that no one has inventoried since they were first deployed.

Third, cloud platforms and SaaS applications are building their own PQC roadmaps. That means RFPs, customer surveys and audit reports will increasingly ask for cryptographic agility - the ability to replace algorithms without rewriting applications. The window to move from reactive to proactive is closing.



03 | Enterprise impact

Imagine a multinational pharmaceutical company with a twenty-year patent portfolio and years of clinical-trial data. Patient records, genomic sequences, regulatory filings and intellectual property are routinely encrypted at rest and in transit. That data may need to stay confidential for 20 to 30 years. An adversary collecting traffic today could hold a decryption-ready library when Q-Day arrives.

The transition touches every layer. Code-signing pipelines, TLS endpoints, key-management systems, Hardware Security Modules and document-signing infrastructure will all need to support new algorithms and larger keys. This is a multi-year, cross-functional initiative, not a security patch.

04 | What CXOs should do

1. Start with economics, not models. Define the business outcome, acceptable error rate, latency requirement and maximum cost per transaction before selecting technology.
2. Build a model portfolio. Use frontier models where they create differentiated value and smaller, specialised or open models for simpler workloads.
3. Establish an AI evaluation layer. Measure accuracy, groundedness, safety, latency and cost continuously.
4. Own the enterprise knowledge and control plane. Keep curated data, retrieval, policies, prompts, evaluation datasets, workflow logic and observability under enterprise control.
5. Scale by evidence. Move from pilot to production only when a use case shows measurable business value, acceptable risk and sustainable unit economics.

05 | The 2027 prediction

By the end of 2027, at least one Fortune 100 CISO will name a cryptographically relevant quantum computer as a Tier-1 enterprise risk in an SEC 10-K filing, and that declaration will stand unchallenged.

“Cryptographic debt is the only technical debt an adversary can choose to collect on at any time.”

The CXO checklist

Three questions for your leadership team

1. If an adversary has quietly collected our encrypted traffic since 2024, which records will they



be able to read in five years, and which still carry commercial or regulatory value?

2. Which systems hold cryptographic keys we cannot rotate without replacing the whole system, and do we know how many such systems we have?
3. Which executive owns this transition, and what number will they put in front of the board next quarter?

One move to make in the next 90 days

Commission a cryptographic inventory across every system that creates or validates digital trust, and put a single-page map of long-lived-data exposure in front of the board before the next strategic planning meeting.



GCSI
GLOBAL CYBER SECURITY INNOVATION
PEOPLE | TECHNOLOGY | RESILIENCE

iblades.ai
safe. effective. secure.
QUANTUM-RESILIENT CYBERSECURITY

CYBERSECURITY FOR WHAT'S NEXT.

INTEGRATE. PROTECT. STAY AHEAD.

GCSI and iBlades bring together cybersecurity expertise and quantum-resilient solutions for a more secure tomorrow.



GuardTron
SECURE THE EDGE
Isolate. Protect.
Keep critical environments safe.



NetTron
THE SOLUTION
Networking and cryptographic security for a connected world.



ManoTron
THE TACTICAL DEVICE
Secure mobility and tactical connectivity.

 GOVERNMENT

 FINANCIAL SERVICES

 HEALTHCARE

 MANUFACTURING

 DEFENCE & AEROSPACE

contact@thegcsi.com | +91 761-9434234 | www.thegcsi.com | www.iblades.ai

SECURE TOMORROW.
ENABLE TOMORROW.



Section 01

04

Cyber Risk / GRC

**Cybersecurity 2027:
From AI acceleration to intelligent
resilience: What CXOs must do now**

Dr. Ram Kumar G

Cybersecurity and Risk Leader, Global Automotive
Company



04 · Cyber Risk / GRC

Cybersecurity 2027: From AI acceleration to intelligent resilience: What CXOs must do now



By **Dr. Ram Kumar G** | Cybersecurity and Risk Leader, Global Automotive Company

Dr. Ram Kumar G is a cybersecurity and risk leader with 20+ years of experience in cybersecurity strategy, governance, risk, privacy, resilience and AI security. He is a LinkedIn Top Voice, industry speaker, mentor and advisory board member, known for translating complex cyber risks into actionable business strategies and advancing responsible AI adoption.



FOCUS

AI governance, third-party and model risk, cyber resilience and continuous controls.

With the emergence of AI-driven threats and defence, cybersecurity is entering a new era. For the past few years, organisations have been busy securing apps, infrastructure, identities and data. By 2027, the greater challenge will be securing how decisions are made and executed in an AI-enabled enterprise.

The question for CXOs is no longer simply, "Are we secure?" It is, "Can we trust the systems that make decisions and take actions on our behalf?"

01 | The Signal

The most important signal is the profound transition from AI as an assistant to AI as a decision-maker.

Generative AI has transformed how employees search, analyse, create and automate. The next wave will see AI-powered systems increasingly connected to enterprise data, applications and workflows and, in some cases, empowered to act autonomously.

This creates a fundamental shift in the cybersecurity equation.

An employee using AI to write an email is one thing. An AI agent that can access customer information, initiate transactions, adjust configurations or make business decisions is another.

At the same time, threat actors are leveraging AI to accelerate reconnaissance, social engineering, vulnerability discovery and fraud. The advantage will increasingly go to the organisations that can combine AI speed with the discipline of security and governance.

We will also see cybersecurity expand beyond the traditional IT perimeter. Third-party AI services, models, agents, data sources and software components will become part of the extended enterprise technology ecosystem.



02 | Why now

Three developments make 2026-27 a defining period.

1. AI adoption is moving from experimentation to enterprise deployment. Organisations are no longer questioning whether they should adopt AI; they are embedding it in customer service, software development, finance, HR, operations and decision-making.
2. Regulation and accountability are catching up. Regulators and policymakers worldwide are raising the bar on transparency, privacy, safety, accountability and the risks of automated decisions. Boards will increasingly need to demonstrate not just AI use but responsible AI use.
3. The attack surface is growing faster than traditional security approaches. Every new AI application, agent, model, integration and data source introduces yet another dependency to manage.

This means cybersecurity is no longer solely a technology issue. It is becoming a business resilience and digital trust issue.

03 | Enterprise impact

The impact will be strongest on organisations that implement AI quickly without redesigning their controls.

Consider a financial institution deploying an AI agent to support credit decisions. The agent might use internal customer data, external data and third-party AI services, while the underlying model or data sources change over time.

Now, suppose a customer challenges the decision and asks a simple question: "Why did I get that credit limit?"

If the organisation cannot reconstruct the information, model logic, rules and approvals that informed the decision, it has a much larger problem that extends far beyond cybersecurity.

It becomes a problem of trust, regulatory compliance, reputation and even financial liability.

The same applies across retail and technology. In sectors such as automotive and healthcare, the implications extend further because AI-driven decisions can affect physical and life safety. As AI becomes embedded into business processes, organisations will need to demonstrate who or what made a decision, what information it used, what controls were applied and who was ultimately responsible.

04 | What CXOs should do

1. CXOs do not need another 100-page AI policy. They need a practical operating model.
2. Clarify accountability: Every material AI use case should have an identified business owner. "AI decided" should not be an acceptable answer.
3. Map out the AI ecosystem: Know which AI models, agents, applications, data sources and third parties are being used across the organisation, including unofficial or "shadow" AI.
4. Prioritise AI according to business impact: Not every AI solution deserves the same level of controls. A marketing-content assistant and an AI that makes financial or safety-critical decisions do not merit the same risk treatment.



5. Integrate security into AI adoption from day one: Privacy, access control, data protection, testing, monitoring, resilience and human oversight should be built into AI workflows, not appended to them.
6. Test AI explainability: Test your organisation's ability to explain the decisions made by an AI system. If you cannot explain this today, then it will be even more difficult when AI starts to operate autonomously at scale.

05 | The 2027 prediction

My forecast is that 2027 will be the year in which organisations stop measuring AI maturity solely by adoption and begin measuring it by trust.

The organisations with the most AI will not necessarily win. It is those with the ability to confidently answer these questions:

1. Where is AI being used?
2. What does it have access to?
3. What can it decide?
4. What can it act on independently?
5. Who is ultimately responsible?
6. Can we prove what happened when a decision goes wrong?

AI governance will become embedded in cybersecurity, enterprise risk and business resilience rather than treated as a separate compliance exercise.

The greatest competitive advantage for the AI-enabled enterprise will not simply be AI prowess. It will be AI that the enterprise can trust, explain and defend.

2027 will be the year enterprises transition from "AI adoption" to "AI accountability."

"2027 will be the year when enterprises stop measuring AI maturity by adoption, and start measuring it by trust."

The CXO checklist

Three questions for your leadership team

1. Where is AI making decisions or taking actions today, and do we know exactly where it has access to our data, systems and processes?
2. For every high-impact AI system, can we clearly identify who is accountable for its decisions, risks and outcomes?
3. If an AI-driven decision is challenged tomorrow, can we reconstruct what happened, why it happened and prove that appropriate controls were in place?

One move to make in the next 90 days

Develop an enterprise AI accountability map - inventory AI use cases including Shadow AI and third-party AI, classify them by business impact, assign accountable owners, and identify the minimum security, privacy, human-oversight and auditability controls required for each.



Section 01

05

Privacy

Governing AI before AI governs
the enterprise

Sandeep Vijayaraghavan

EVP, Cybersecurity & Cloud | Terralogic

05 · Privacy

Governing AI before AI governs the enterprise



By **Sandeep Vijayaraghavan** | EVP, Cybersecurity & Cloud | Terralogic

Sandeep Vijayaraghavan is a cybersecurity and AI security leader with experience building and scaling consulting and services businesses across SOC, cloud, data, identity, application and OT security. His work focuses on helping enterprises adopt AI securely through practical guardrails, governance and security by design.



FOCUS

AI governance, Digital workers, Identity and authority, Secure autonomy, Continuous assurance

01 | The Signal

Enterprise AI is crossing a critical threshold. It is moving from assisting employees with content and analysis to acting inside business processes: reading sensitive data, invoking tools, writing code, making recommendations and initiating transactions. At this point, AI is no longer only a productivity platform. It is becoming a new enterprise attack surface and, increasingly, a new class of digital operator.

The first wave of AI adoption was easy to see: public chatbots, isolated pilots and controlled experiments. The next wave will be much harder to govern. AI will be embedded in applications, SaaS platforms, development environments, contact centres, finance workflows and operational systems. Some deployments will be approved; many will arrive through features switched on by vendors or tools adopted directly by business teams.

This creates two simultaneous shifts. Threat actors are using AI to scale reconnaissance, social engineering, impersonation and malware adaptation. At the same time, enterprises are giving AI systems access to valuable data and the ability to act. The larger risk is not that an AI model produces one incorrect answer. It is that an AI-enabled workflow makes an untrusted decision at machine speed, using privileged access, without adequate visibility or accountability.

02 | Why now

AI adoption is moving faster than the controls designed to govern it. Boards are asking for measurable AI returns, business teams are under pressure to deploy, and technology providers are adding copilots and agents across the enterprise stack. The result is an expanding estate of models, prompts, plug-ins, retrieval stores, agents, APIs and machine identities, often without a reliable enterprise inventory.



The threat model has also changed. Prompt injection can manipulate an AI system through apparently legitimate content. Sensitive data can leak through prompts, logs, embeddings or generated output. Poisoned documents can corrupt retrieval systems. Compromised models, libraries or third-party services can introduce supply-chain risk. Excessive agency can allow an AI system to take actions beyond the user's intent. Weak output handling can turn generated content into executable risk. These are no longer theoretical categories; they are design conditions that enterprises must expect.

Traditional cybersecurity assumed a relatively clear boundary between a human user, an application and a controlled action. Enterprise AI blurs that boundary. An agent may act for a person, call another agent, use a service account, query multiple data sources and execute through an API. It can be difficult to determine whose authority was used, which data influenced the decision, and who is accountable when the outcome is wrong.

Responsible AI therefore cannot remain a statement of principles owned only by legal, ethics or data-science teams. Fairness, transparency, privacy, robustness and human oversight must be translated into technical controls and operating accountability. AI governance must answer practical questions: Which systems exist? What decisions can they influence? What data and tools can they access? How are they tested? Who can stop them? What evidence is retained for audit and incident response?

03 | Enterprise impact

At enterprise scale, cybersecurity and AI governance converge around four control problems.

Identity and authority. AI agents and non-human identities may soon outnumber human users in important digital workflows. Each agent needs a defined owner, a unique identity, least-privilege access, short-lived credentials and explicit transaction limits. An agent should never inherit broad authority simply because the human who configured it has that authority.

Data and context. AI systems do not use only structured databases. They consume documents, conversations, vector stores, external content and real-time context. Data classification, consent, residency, retention and access policies must follow the information into prompts, retrieval pipelines and generated outputs. A secure model connected to poorly governed data is still an insecure system.

Action and autonomy. The risk rises sharply when AI moves from recommending to executing. A customer-service assistant that drafts a response is different from an agent that changes an account, approves a refund or creates a beneficiary. High-impact actions require deterministic policy checks, separation of duties, transaction thresholds and human approval that cannot be bypassed by the model.

Assurance and accountability. Models change, prompts change, enterprise data changes and attacker behaviour changes. A system that passed testing at launch may drift into unsafe behaviour. Enterprises need continuous evaluation, red teaming, behavioural monitoring, traceable decision logs and an incident process built for AI-specific failures. Governance must operate throughout the lifecycle, not at a one-time approval gate.

The operating model will change as well. The CISO cannot own AI risk alone, and an AI council



cannot govern systems it cannot see. Business owners must remain accountable for outcomes; technology teams for architecture and reliability; data leaders for information use; legal and compliance teams for obligations; and security teams for threats, control assurance and response. The board's role is to set risk appetite and require evidence that AI value is being created within it.

04 | What CXOs should do

1. Create one enterprise AI register. Inventory every AI use case, model, agent, data source, external provider, integration and accountable owner. Include embedded vendor features and employee-adopted tools, not only centrally funded programmes.
2. Tier AI by impact and autonomy. Classify systems by the sensitivity of their data, the consequence of their decisions and their ability to act. Apply stronger controls as autonomy and business impact increase.
3. Govern the whole AI system. Assess prompts, retrieval data, model provenance, plug-ins, APIs, machine identities, memory, output handling and human hand-offs. Model approval alone does not secure the workflow.
4. Put policy outside the model. Use identity controls, allow-listed tools, transaction limits, data-loss prevention, deterministic validation and approval workflows to enforce boundaries. Never rely on a system prompt as the primary security control.
5. Continuously prove trustworthiness. Test for prompt injection, data leakage, poisoning, unsafe outputs, bias, drift and excessive agency before release and during operation. Monitor both technical behaviour and business outcomes.
6. Prepare for AI incidents. Extend incident response to include disabling agents, revoking machine credentials, isolating retrieval sources, preserving prompts and decision traces, notifying stakeholders and restoring a known-safe configuration.

05 | The 2027 prediction

By 2027, leading enterprises will manage AI agents as governed digital workers. Every material agent will have an owner, an identity, a defined purpose, bounded access, an approved action set and a measurable risk posture. Organisations that cannot answer what their AI can see, decide and do will discover that scale without governance does not create intelligence; it creates unmanaged operational power.

"The enterprise risk is not AI making a mistake. It is AI acting with authority before governance can intervene."

The CXO checklist

Three questions for your leadership team

1. Can we identify every material AI system and the executive accountable for its outcomes?
2. Do we know what data, identities and tools each AI system can access, and what actions it can take?
3. Can we detect unsafe behaviour, stop the system quickly and reconstruct why a decision was made?

One move to make in the next 90 days

Frameworks informing this outlook: NIST AI Risk Management Framework and Generative AI Profile; OWASP Top 10 for LLM and Generative AI Applications 2025; MITRE ATLAS.



Section 01

06

Talent and skilling

The half-life of expertise:
How AI is rewriting technology talent

Dr. Shinu Abhi

Director, Corporate Training | REVA Academy for
Corporate Excellence, REVA University

06 · Talent and skilling

The half-life of expertise: How AI is rewriting technology talent



By **Dr. Shinu Abhi** | Director, Corporate Training | REVA Academy for Corporate Excellence, REVA University

Dr Shinu Abhi is a Fulbright Fellow and technology-education leader with 25 years across higher education and industry. Her work spans business analytics, AI systems, cybersecurity governance, enterprise skilling and customised technology programmes for working professionals and organisations.



FOCUS

Perishable expertise, skills-based organisations, AI-augmented professionals, project evidence and human judgement.

01 | The Signal

For most of the last three decades, a technology professional's value compounded. A skill learned early - a language, platform or framework - could pay dividends for a decade or more. That assumption is breaking. The expertise that defines a role today has a shorter usable life than at any point in the industry's history, and the curve is getting steeper. When an AI system can write competent code, draft a threat model or configure infrastructure in seconds, the value of any single technical skill drops fast. What rises instead is the value of knowing which skill to apply, and whether the machine got it right. You are no longer managing a workforce whose skills appreciate. You are managing one whose skills depreciate, and whose judgement appreciates.

02 | Why now

Three forces have converged in 2026 and 2027. First, generative and agentic AI have moved from novelty to daily tools inside engineering, security and analytics teams. The productivity floor has risen, but so has the rate at which yesterday's specialised skill becomes today's commodity. Second, the supply of AI-augmented output has outpaced the supply of people trained to supervise it. Enterprises now have more machine work than they have human judgement to check it. Third, the credential system organisations relied on to signal competence - certifications, degrees and years of experience - now lags the technology by design. It certifies knowledge that can age before the ink is dry. The result is a widening gap between what people were hired to know and what the work actually needs, and hiring alone cannot close it.

03 | Enterprise impact

The impact falls first on cost and capability, and it is uneven. In technology services, when AI compresses the effort behind routine development and testing, the pyramid that made scale profitable starts to invert. Fewer junior hands can produce the same output, but far more experienced judgement is needed to review, secure and stand behind what the machine produces.



The scarce resource is no longer headcount; it is people who can direct and audit AI.

Operating models feel it next. Fixed job descriptions such as Java developer, SOC analyst or data engineer become poor descriptions of what people actually do, which is increasingly about orchestrating and verifying AI systems across domains. Firms adapting fastest are moving from role-based to skills-based structures, where work is assembled from capabilities rather than titles. The professional who is deep in one domain but literate across several becomes more valuable because that breadth is exactly what AI still struggles to supply reliably.

04 | What CXOs should do

1. Measure the half-life, not the headcount. For each critical technology function, estimate how much of its core skill set AI could automate within 24 months.
2. Shift from certification to evidence. Value what a person has demonstrably built, secured or shipped over credentials that certify ageing knowledge.
3. Build for depth and breadth, on purpose. Fund deep expertise in one domain plus working fluency across two or three adjacent domains.
4. Protect and price human judgement. Name the decisions that must stay human and invest in the people who make them well.
5. Make learning continuous and funded. Treat reskilling as infrastructure, with dedicated time, budget and a cadence that matches technology change.

05 | The 2027 prediction

By 2027, leading enterprises will hire and promote on demonstrated, project-based evidence of capability rather than on certifications or years of experience. AI-augmented judgement will appear as an explicit, assessed competency in technology job descriptions.

"You are no longer managing a workforce whose skills appreciate. You are managing one whose skills depreciate, and whose judgement appreciates."

The CXO checklist

Three questions for your leadership team

1. For our most critical technology roles, how much of today's core skill set will AI make routine within 24 months, and do we actually know?
2. Are we promoting people for what they can demonstrably build and secure, or for what their certificates say they know?
3. Which decisions in our organisation should never be handed to a machine, and are we investing in the people who make them well?

One move to make in the next 90 days

Pick one critical function - engineering, security or analytics - and run a skills half-life audit. Map its core skills against what AI can already do, and publish a 12-month reskilling plan tied to project evidence, not course completion.



Section 01

07

AI readiness and ROI

80/20, inverted:
Closing the AI readiness gap

Krishna Pandey

CISO, PropertyGuru Group



07 · AI readiness and ROI

80/20, inverted: Closing the AI readiness gap



By **Krishna Pandey** | CISO, PropertyGuru Group

With nearly two decades of experience across Xerox, Salesforce, Citrix, Cloudera, formerly Hortonworks, and C-DAC R&D, Krishna Pandey has scaled GCC security programmes, led critical-risk reduction for Fortune 100 organisations and pioneered AI security frameworks. He served as President of the ISC2 Bangalore Chapter from 2019 to 2022 and speaks frequently in India, Europe and the United States.



FOCUS

Why AI's ROI problem isn't a technology problem and what the organisations already getting a return are doing differently.

01 | The Signal

During 2026, the boardroom AI conversation quietly changed. For two years the question was how fast an organisation could adopt AI. Now it is where the return actually is - and for most enterprises, there still is not a good answer. MIT Project NANDA's 2025 study reported that 95% of enterprise generative AI pilots delivered no measurable P&L impact. The 2026 evidence points in the same direction: McKinsey reports that 37% of respondents attribute at least some EBIT impact to AI and only 6% qualify as AI high performers; PwC finds that the top 20% of organisations capture 74% of AI-driven returns; BCG identifies only 6% of companies as AI leaders; and Gartner reports that only 28% of AI use cases in infrastructure and operations fully meet ROI expectations. The conclusion is not that AI lacks value. It is that value depends on the operating system around the model - data engineering, governance, workflow integration, measurement and change management - the unglamorous plumbing that many pilots were never funded to build.

02 | Why now

Three forces are converging on the same budget cycle. First, capital: major hyperscalers are projected to spend roughly \$675 billion on AI infrastructure in 2026, raising the bar for measurable returns. Second, value is concentrating in a small group of organisations that are redesigning workflows and operating models rather than layering AI onto existing processes. Third, readiness still lags adoption: McKinsey reports that only about one-fifth of organisations have fundamentally redesigned their operating models around AI. That missing operating readiness - the data, governance, process ownership, measurement and skills behind the model - is the real gap. In 2026, that omission is becoming too expensive to ignore.



03 | Enterprise impact

The impact shows up first in cost and operating model, not in the model itself. The same 2026 research finds a consistent pattern: AI cuts a task from ten days to one, but the customer still waits ten days, because nobody redesigned the process around the faster step. The saving never reaches the P&L; it gets reabsorbed by a workflow still built for the old pace. That is what the missing 80% actually costs, not one dramatic failure, but hundreds of small, funded, invisible ones, each quietly absorbed back into the org chart it was meant to change.

The same gap shows up in talent and risk. Enterprises are standing up AI agents and service accounts faster than they can govern them - a population that barely existed eighteen months ago, still managed by processes built for annual reviews. The risk is no longer theoretical. During internal cybersecurity evaluations in July 2026, OpenAI models circumvented controls and compromised parts of Hugging Face's systems. Most CXOs will never see an incident at that scale, but many already carry the same underlying ingredients: over-permissioned identities, weak isolation and insufficient monitoring.

04 | What CXOs should do

1. Fund the boring 80%. Treat the 10/20/70 split as a planning heuristic: roughly 10% of effort on algorithms, 20% on data and technology, and 70% on people, process and workflow redesign. Pair every AI budget line with governance and measurement, rather than adding them after something breaks.
2. Redesign the workflow; do not bolt AI onto it. AI high performers are far more likely to fundamentally redesign workflows than other organisations. Decide where the work lives and who - human or agent - owns each task before choosing the tool.
3. Govern AI identities like privileged human ones. Move agents and service accounts off standing, long-lived credentials onto short-lived, task-scoped access with a named accountable owner, before an audit or an incident forces the question.
4. Concentrate, do not scatter. A focused portfolio of deeply resourced AI use cases is easier to measure, govern and scale than a wide field of loosely funded pilots.
5. Report readiness to the board, not just adoption. Usage and seat counts are easy to generate and easy to fake; a board that only sees adoption metrics cannot tell real value from a well-funded demo, and neither can you until an auditor or a credit analyst does it for you.

05 | The 2027 prediction

By late 2027, the first Fortune 500 board may replace a CXO after a sensitive-data leak or customer-trust breach traced to an ungoverned AI agent. The failure will be one of access control, not the model, making AI engineering and its underlying infrastructure central to boardroom discussions.

"AI has a frog to eat, and it isn't the model; it's the plumbing. Skip it, and the bill arrives with interest."



The CXO checklist

Three questions for your leadership team

1. Can we point to a specific P&L line each AI initiative has moved, not adoption, not sentiment, a number the CFO would sign off on?
2. Have we funded the unglamorous 80%, data, governance, measurement, ownership, as seriously as the AI licence itself?
3. Can we govern and run our AI systems safely at the speed they actually operate, not the speed of last year's compliance review?

One move to make in the next 90 days

Pick one AI initiative already in flight: name the P&L line it must move, fund the unglamorous plumbing behind it, data, governance, measurement, and stand up the governance plan that keeps it running safely before you fund a second.

TSMT
INTELLIGENCE X COMPOUNDED

AI Transformation Advisory in Business Process and Finance

Making business simpler, faster and smarter.

- Fractional CAIO**
Optimise your AI Function
- Workflow Automation**
Routine work, off your desk
- Assisted Realtime MIS & Business Metrics Dashboard**
with live analytics agents
- Extraction, Connectors and Calculators**
for all your complex analytics and manual tasks.

**PEOPLE
TECHNOLOGY
FINANCE
A BRIGHTER
TOMORROW**

50 Years of Trust. Built for Tomorrow.

WWW.TSMTCONSULTING.COM

STRATEGY TO OUTCOMES | PEOPLE EMPOWERED | TECHNOLOGY THAT DELIVERS | SUSTAINABLE GROWTH | vinayt@tsmt.in | 9986079182



Section 02

The CXO agenda

10 questions every CXO should ask before 2027

A boardroom conversation starter, designed to be photographed, shared and debated.

01

Where are autonomous AI agents already making decisions in my organisation?

06

Do we know the cost of every AI inference or workload?

02

Can we identify every cryptographic dependency in our enterprise?

07

Can our security operations defend against machine-speed attacks?

03

What percentage of our AI experiments have reached production?

08

Which jobs will materially change because of AI in the next 24 months?

04

What happens if our primary LLM or inference provider becomes unavailable?

09

Which technology capabilities must we own internally?

05

Which enterprise data should never enter a public AI model?

10

What technology bet would we regret not making by 2027?



Section 03

RACE alumni in action

In their own words, ten alumni share how RACE shaped their careers, confidence and leadership journeys.



Naresh Choudhary

Senior Vice President, Quality and Productivity · Infosys

M.Tech in Cybersecurity · 2025

"RACE has reignited my hunger for knowledge and learning. It helps me keep myself and my team ahead in emerging technology and business areas. I also recently co-authored Powering Enterprise DevSecOps with colleagues, capturing the lessons from our experience over the years."



Ganesh Subramanian

Delivery Manager, Enterprise Productivity and Engineering Excellence · Infosys

M.Tech in Artificial Intelligence · 2023

"RACE helped me build on my industry experience with a deeper understanding of AI and its practical applications. The M.Tech programme strengthened my confidence to move from technology practice into research, leading me to pursue a PhD in AI-driven cybersecurity and bring a more analytical, evidence-based approach to professional challenges."



Mallikarjuna Bande

Director, Design Enablement and Digital Transformation · NXP Semiconductors

M.Tech in Artificial Intelligence · 2024

"The RACE programme laid the foundation for my transformation into AI. Its blend of academic rigour and industry relevance empowered me to apply AI beyond my core expertise. Today, I drive AI-led innovation and digital transformation in the semiconductor and VLSI domain."



Ashok Shetty

Senior Vice President, Underwriting Analytics and Data Science · Swiss Re Corporate Solutions

MBA in Business Analytics · 2020

"The RACE Business Analytics programme transformed the way I approach business and decision-making. It strengthened my analytical mindset, leadership capabilities and confidence, while giving me practical exposure to real-world challenges. It helped me turn data into actionable insights and lead with greater clarity, ownership and strategic thinking."



Anuraag Anand

Vice President · Accenture

MBA in Business Analytics · 2022

"RACE helped me transition from managing delivery outcomes to leading with greater strategic intent. It strengthened my executive presence, broadened my enterprise perspective and enabled me to influence stakeholders beyond my immediate responsibilities. The programme gave me greater confidence to lead transformation and embrace AI-led innovation."



RACE alumni in action

From learning to enterprise impact



Manoj Tayde

Senior Technical Lead · Aziro, formerly MSys Technologies

M.Sc in Cloud Architecture and Security · 2025

"Completing my master's at RACE strengthened my technical expertise and broadened my perspective on cloud technologies, architecture and security. The programme helped me connect theory with real-world challenges, build confidence in architectural decision-making and accelerate my transition towards technology leadership and architecture roles."



Joy V. Ramachandran

Head of Transformation and Innovation, Operational Automation and AI CoE · SAP

M.Tech in Cybersecurity · 2022

"RACE broadened my perspective beyond technical expertise and strengthened my strategic thinking, leadership and understanding of emerging technologies. Its industry-relevant curriculum and experienced faculty encouraged continuous learning, innovation and adaptability. Publishing my research paper was a significant personal achievement that further enhanced my professional growth."



Sivakumar Dhakshinamoorthy

Head of Service Support · Lenovo

M.Sc in Cybersecurity · 2020

"RACE and my master's in cybersecurity strengthened my ability to engage confidently with CXOs on product security and cyber resilience. The programme enhanced my strategic leadership perspective, helping me bridge technology, risk and business priorities while driving transformation in an increasingly digital and AI-driven landscape."



Paul Vettukallel

Lieutenant Colonel · Indian Army

M.Sc in Artificial Intelligence · 2025

"The programme at RACE was the right foundation for me to understand and explore the mathematical principles on which AI models are built. It helped me grasp how different concepts work together, from learning Python from scratch to contributing actively to AI adoption and transformation in the Indian Army."



R. Thogaivani

Scientist F · Aeronautical Development Establishment, DRDO

M.Tech in Artificial Intelligence · 2024

"RACE was a catalyst for my professional transformation, enabling me to combine experience in flight simulator development, systems engineering and project management with advanced AI capabilities. I now contribute to speech-to-text for pilots' comments, aerial-image object detection and AI-assisted mission debriefing for next-generation defence technologies."



Section 04

The RACE ecosystem

How RACE is building technology leaders for 2030

Not a programme brochure, but a view of the capability system behind the Outlook.



Learn

Executive master's, diploma and certification programmes for working professionals.



Build

Capstones, labs and proof-of-work: learning that ships.



Solve

Enterprise consulting and applied projects with industry.



Research

Industry research and publications, including this Outlook.



Connect

The CXO ecosystem includes RACEx360, roundtables and communities.



RACE, REVA University

Working at the intersection of emerging technology, executive learning and enterprise application across AI, cybersecurity, cloud, analytics and technology leadership.



Section 05

Partners

RACEx360 2026 partner recognition

With thanks to our RACEx360 2026 partners.

TITLE SPONSOR



PLATINUM SPONSOR



GOLD SPONSOR



docker

NUTANIX

SILVER SPONSOR



ASTRIKOS



ASSOCIATE SPONSOR



**CARE POINT
TECHNO SOLUTION
PVT. LTD.**



**VISIMINDS
TECHNOLOGIES**



CleanStart



TigerGate

Utkrusht

SEMINAR



**DataNex
Analytics
Solutions**



Contributors

The people behind the Outlook

Practitioner perspectives shaping the 2026–27 Outlook.



Dr. Jay B. Simha | CAIO, adoptAI Technologies |
Chief AI Mentor, RACE, REVA University

AI and analytics leader with 20+ years across telecom, BFSI, manufacturing and enterprise applications. A Ph.D. in AI, his current research and consulting focus on Frugal AI, decision systems and enterprise value.



Pradeepta Mishra | VP, AI, Beghou

Senior AI leader, author, inventor and educator with more than two decades of experience in AI, machine learning and data science. He has 17 patents, 11 books and extensive experience translating AI into enterprise applications.



Sridhar Govardhan | Group CISO, Angel One

Technology and cybersecurity leader with experience across IT/ITES, e-commerce, Web3 and financial services. He leads cybersecurity and risk strategy at Angel One, with emphasis on innovation, responsible AI, customer trust and business resilience.



Dr. Ram Kumar G | Cybersecurity & Risk Leader, Global Automotive Company

Cybersecurity and risk leader with 20+ years across strategy, governance, privacy, resilience and AI security. He is an industry speaker and mentor focused on translating complex cyber risk into actionable business decisions.



Contributors

The people behind the Outlook

Practitioner perspectives shaping the 2026–27 Outlook.



Sandeep Vijayaraghavan | EVP, Cybersecurity and Cloud, Terralogic

Cybersecurity and AI security leader with experience building and scaling consulting and services businesses across SOC, cloud, data, identity, application and OT security. His work focuses on practical guardrails, governance and security by design.



Krishna Pandey | CISO, PropertyGuru Group

Senior AI leader, author, inventor and educator with more than two decades of experience in AI, machine learning and data science. He has 17 patents, 11 books and extensive experience translating AI into enterprise applications.



Dr. Shinu Abhi | Director, Corporate Training, RACE, REVA University

Fulbright Fellow and technology-education leader with 25 years across higher education and industry. Her work spans business analytics, AI systems, cybersecurity governance, enterprise skilling and customised technology programmes for working professionals and organisations.



How to read this Outlook

RACE foresight method

A practical framework for turning technology signals into executive decisions.

This edition combines practitioner-authored outlooks with RACE's enterprise learning, consulting and CXO engagement perspective. The aim is directional judgement rather than false precision. Each technology is considered through four lenses:



Enterprise Readiness

Can a typical enterprise deploy it reliably with available skills, architecture and controls?



Business Impact

If adopted well, how materially could it change cost, growth, risk, speed or operating model?



Adoption Horizon

Is the leadership action to scale now, pilot now, build capability, or simply watch?



Risk × Reward

Where does the upside justify controlled experimentation, and where should enthusiasm be tempered by uncertainty?



Take it to the boardroom

My 90-day technology agenda

Use this page after RACEx360. Five decisions. One quarter.

01

One technology we should scale now

02

One experiment we should run

03

One capability we must build internally

04

One risk we are underestimating

05

One decision I will take to the next leadership meeting





ONE PLATFORM. INFINITE POSSIBILITIES.

Connect. Analyze. Predict. Act.

Intelligent Operations.
Real-Time Decisions.



Smart Cities
Safer. Greener. Smarter Communities.



Smart Buildings & Campuses
Efficient Spaces. Better Experiences.



Smart Transport & Infrastructure
Connected Mobility. Smarter Infrastructure.



Industry 4.0 & Manufacturing
Smarter Operations. Higher Productivity.



Energy, Utilities & Critical Infrastructure
Reliable Resources. A Resilient Tomorrow.



Data Centers
Higher Availability. Greater Efficiency.



Defence & Protected Markets
Mission Ready. Secure Futures.

AI-POWERED PLATFORM FOR INTELLIGENT OPERATIONS



Real-time Analytics & Predictions



Intelligent Insights & Recommendations



Automated Actions & Workflows



Visualisation & Digital Twin



Agentic AI



Secure / Scalable / Interoperable. Cloud / On-prem

connect@astrikos.ai | +91 74065 54000 | astrikos.ai

LET'S BUILD A SMARTER, MORE CONNECTED TOMORROW.

ONE PARTNER. SIX PILLARS.



Integrated IT solutions for a smarter, safer and stronger enterprise.

We design, deploy and manage resilient infrastructure and innovative solutions that power your business today and make it ready for tomorrow.

About Us

For 35 years, we've helped organisations across 33 countries stay connected, secure and ahead of the curve.

From enterprise infrastructure to emerging technologies, we deliver end-to-end IT solutions with accountability, agility and expertise at the core.

23+ YEARS | 647+ COUNTRIES | 33 COUNTRIES | \$30M+ REVENUE

Our Capabilities

- IT Infrastructure**
Enterprise networking, data centre, storage, and compute.
- Managed Services**
24/7 AOC & SOC monitoring, Cloud Managed Edge.
- Cloud & Software**
Cloud migration, platform development, API integration.
- Intelligent Managed Service**
Proactive monitoring, SLA-backed NOC/SOC, Managed intelligence.
- Emerging Tech**
AI, IoT, intent-based networking, cybersecurity.
- Professional Services**
Help desk, field operations, advanced consulting.

AI Security at the Core

We embed AI-powered security across our solutions to detect threats faster, respond smarter and keep your business always protected.

- AI-Powered Threat Detection
- Proactive Response
- Continuous Monitoring
- Enterprise-Grade Protection



CAREPOINT
TECHNO SOLUTION PVT. LTD.
PEOPLE | TECHNOLOGY | PROGRESS

A SMARTER TOMORROW TOGETHER

SECURE YOUR BUSINESS. TRANSFORM YOUR FUTURE.

End-to-end IT solutions that drive performance, strengthen security and create new possibilities for your business.

IT for a Smarter Tomorrow



COMPLETE IT SOLUTIONS UNDER ONE ROOF

- COMPUTE**
Powering performance for modern workloads.
- STORAGE**
Secure, scalable and always available.
- NETWORKING**
Connect, collaborate and grow.
- SECURITY**
Protection for today. Readiness for tomorrow.

POWERED BY LEADING TECHNOLOGY PARTNERS

Hewlett Packard Enterprise | hp | aruba | Microsoft | Red Hat

www.carepoint-india.com | +91 93865 70099 | helpdesk@carepoint-india.com

Technology That Drives Business Forward



REVA Academy for
Corporate Excellence

IN PARTNERSHIP WITH
 **CISO**



REVA
UNIVERSITY
Bengaluru, India

REVA Academy for
Corporate Excellence (RACE)

Built for working professionals

Learn. Apply. Lead. Transform.

RACE is the industry-focused learning and consulting arm of REVA University. We help working professionals and organisations build capabilities in emerging technologies, leadership and digital transformation.

**Learning
designed around
your career**

Industry-led.
Practice-driven.
Outcome-focused.



What we offer

Master's programmes

Weekend MTech/MSc programmes in AI, Cybersecurity, Cloud Architecture and Security, Business Analytics

Short-term programmes

Focused learning from three days to three months, designed for rapid upskilling and career advancement.

Applied learning and labs

Hands-on learning through GPU-powered labs, the Security Operations Centre, Cyber Range and enterprise capstone projects.

Corporate programmes

Customised capability-building solutions aligned with business priorities, roles and transformation goals.

Projects and product development

Turn real-world challenges into working solutions through guided projects, prototypes and product development.

Build capabilities that create enterprise impact

Explore our programmes, corporate solutions and learning experiences.



Scan here to
discover more.



RACE, REVA University
Kattigenahalli, Yelahanka,
Bangalore, 560 064

+91 89040 58866
race@reva.edu.in
www.race.reva.edu.in



NAAC
GRADE **A+**
ACCREDITED UNIVERSITY

REVA
UNIVERSITY
Bengaluru, India

GREAT IDEAS DON'T BELONG TO ONE DISCIPLINE

NEITHER SHOULD YOUR EDUCATION

AT REVA UNIVERSITY,
multidisciplinary learning
empowers students to
collaborate, innovate, and
create meaningful impact

THIS IS HOW WE EDUCATE TO ENTERPRISE



Rukmini Knowledge Park, Kattigenahalli
Yelahanka, Bengaluru - 560 064
Karnataka, India.

Ph: +91 9611201303, +91 9021190211, 080 4696 6966
E-mail: admissions@reva.edu.in

Follow us on

[/revauniversity_official](#) [/REVAUniversity](#) [/revauniversity_official](#)
[@revauniversity_official](#) [/REVA University](#) [reva.edu.in](#)
[+91 90211 90211](#)



Your team shouldn't have to do everything.

Let AI handle the work.

AI agents that can understand requests, take action,
and complete business operations across:



HR



IT



FINANCE



PM



CRM

Meet **Blazey**

The AI That Does & Not Just Chats

- Understands the requests
- Chooses the right agent
- Takes actions

And gets the task done.

One Platform, Five AI Agents

Blazeup: The AI that does. Not AI that chats.

Ready to
blaze it up?

Scan to explore more!



Don't just find the risk. Find the path.

FlyView maps the relationships that turn individual findings into meaningful experiences.

The risk isn't always the finding.
It's what the finding connects to.

1

IDENTITY

Who has access?

2

DATA

What can they reach?

3

AI

What can it access or act on?

4

APPLICATIONS + INFRASTRUCTURE

What path connects them?

From isolated findings to **connected exposure.**



For admissions, contact

Phone: +91 89040 58866

For customised programs, contact

Dr. Shinu Abhi | Fulbright Fellow

Director- Corporate Training

REVA Academy for Corporate Excellence (RACE)

Phone: +91 99729 17030

E-Mail: shinuabhi@reva.edu.in



REVA University

Rukmini Knowledge Park Kattigenahalli, Yelahanka,
Bangalore 560 064 Karnataka, India.



race@reva.edu.in



race.reva.edu.in

REVA RACE