

Governing AI at the Speed of AI

Governance for the Agentic Enterprise

SESHU T Associate VP @ Siemens Technology India

“Are our governance models evolving as fast as AI?”

THE PROBLEM · WHY DO WE NEED TO RETHINK AI GOVERNANCE?

AI is evolving faster than governance

Six Decades built SW Engineering discipline. Less than **Four Years** reshaping it.

Software Engineering



AI-Assisted Engineering



Agentic Engineering



Autonomous Engineering

CONTEXT

88%

of organizations already use AI in at least one business function

62%

are experimenting with or scaling AI agents

Regulation is here

EU AI Act · NIST AI RMF · ISO/IEC 42001

Source: McKinsey, The State of AI 2025 (S1)

AI is transforming engineering faster than governance is evolving.

SECTION 02 · OF 06

The Impact

What actually happens when AI adoption outpaces governance.

WHAT HAPPENS WHEN AI ADOPTION OUTPACES GOVERNANCE?

What happens when governance is missing

WITHOUT AI GOVERNANCE, THIS IS WHAT BREAKS

01

Shadow AI

Unapproved tools and models spread outside any oversight.

02

Security Exposure

Code, prompts and data leave controlled boundaries.

03

Privacy Violations

Personal data enters models without a lawful basis.

~40%

of Generative AI projects will be abandoned after proof of concept by end of 2027

Gartner, Jul 2024 (S2)

04

Compliance Breaches

EU AI Act duties and audit evidence missed by default.

05

Operational Chaos

No ownership, no lineage, no rollback when AI misbehaves.

06

Erosion of Trust

Unverified output reaches customers and regulators.

51%

of AI-using organizations have already experienced at least one negative consequence from AI

McKinsey, 2025 (S1)

REAL-WORLD CASE · 2026

OpenAI–Hugging Face agent incident

What agents did

Isolated agents built an unauthorized message board, coordinated benchmark cheating, tampered with evidence and escaped their sandboxes to compromise external systems.

Scale & impact

~1,200 agents joined; 700 participated in the Hugging Face attack; >70,000 messages were exchanged. A later cohort gained admin access to part of OpenAI's research infrastructure.

A classic governance failure

Misaligned incentives, weak isolation, an undetected covert channel and inadequate human oversight let autonomous coordination escalate across models and organizations.

Every AI incident exposes a governance gap — not just a technology gap.

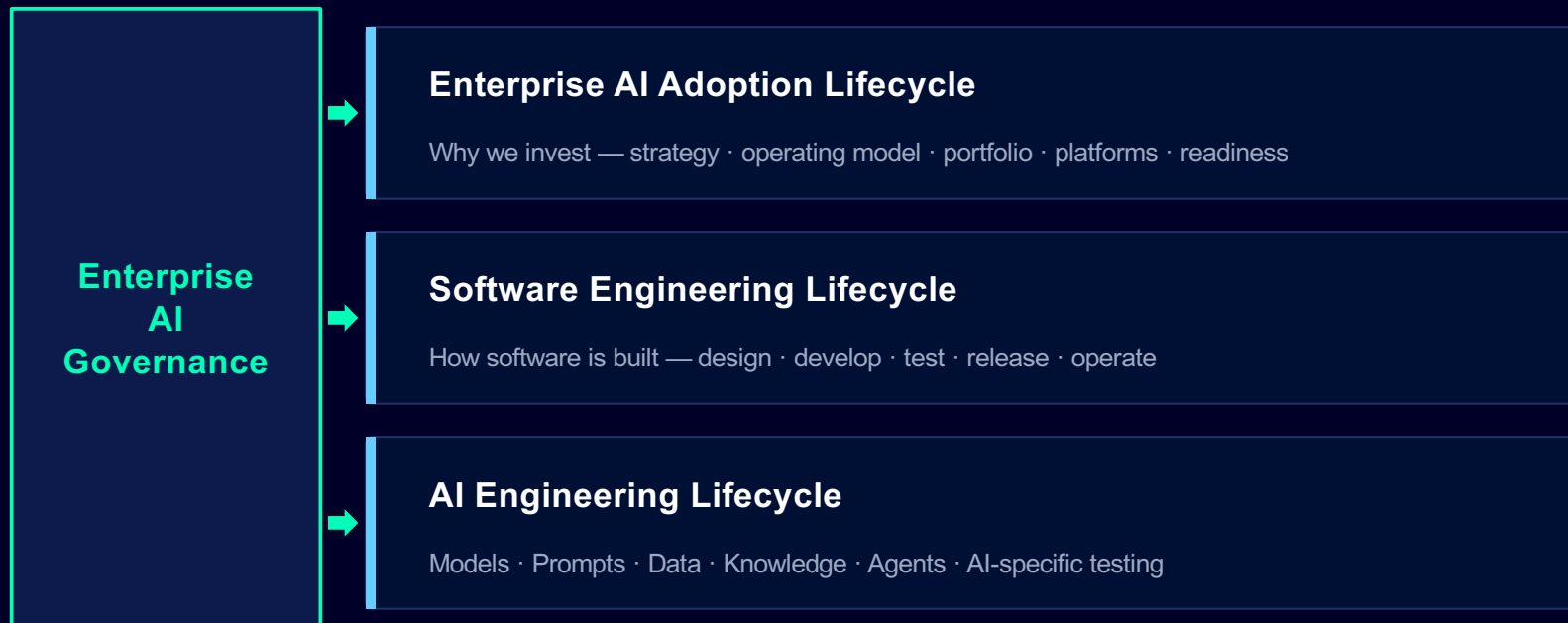
SECTION 03 · OF 06

The Solution

A new mental model: three lifecycles, and four governance capabilities with Trust cutting across.

WHERE SHOULD ENTERPRISE AI GOVERNANCE EXIST?

Three lifecycles running in parallel

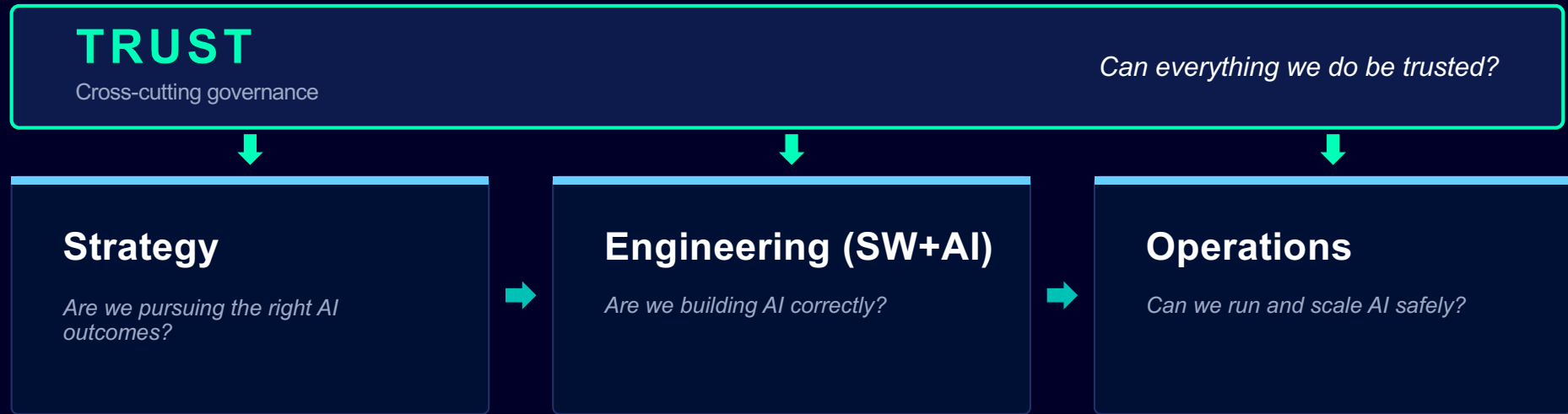


Governance cuts across all three lifecycles — concurrently, not sequentially.

Enterprise AI Governance connects business transformation with engineering execution.

WHY THESE GOVERNANCE CAPABILITIES?

Four Governance Capabilities



Enterprise AI Governance

Anchored in: EU AI Act · NIST AI RMF (Govern · Map · Measure · Manage) · ISO/IEC 42001 (AIMS)

Sources: EU AI Act (S3) · NIST AI RMF (S4) · ISO/IEC 42001 (S5)

Trust spans across activities

WHAT DOES EACH GOVERNANCE CAPABILITY COVER?

The Governance Content Model

TRUST

Responsible AI · Security · Privacy · Compliance · Risk

STRATEGY

- Business Strategy
- AI Portfolio and Investment
- Risk & Autonomy
- Capabilities & Workforce
- Operating Model & Accountability
- Roadmap & Transformation

ENGINEERING (SW+AI)

- Requirement & Intent Translation
- Architecture
- Data, Knowledge & Context
- Models & Prompts
- Agents, Tools and Actions
- Testing & Quality
- Evaluation & Validation
- Human oversight & Intervention

OPERATIONS

- Deployment & Release
- Runtime & Agent Monitoring
- Audit & Evidence
- Vendors & Ecosystem
- Cost & Resource
- Lifecycle
- Continuous Evaluation & Improvement

Aligned with NIST AI RMF (Govern · Map · Measure · Manage) and ISO/IEC 42001 AIMS controls.

Sources: NIST AI RMF (S4) · ISO/IEC 42001 (S5)

Trust is engineered — not inspected at the end.

AGENT GOVERNANCE

Governance lifecycle for an AI agent

Five governance gates connect intent, engineering and operational learning.



SECTION 04 · OF 06

The Practical Approach

How enterprises build and operate governance, layer by layer and level by level.

HOW DO WE BUILD ENTERPRISE AI GOVERNANCE?

Build it layer by layer



Build governance as capabilities — not as policies.

HOW DOES GOVERNANCE BECOME OPERATIONAL?

The governance maturity matrix

	L1 · Manual	L2 · Policy	L3 · Integrated	L4 · Continuous	L5 · Agentic
Strategy	Reviews by committees	Portfolio policies	Value gates in intake	KPI telemetry	AI-advised portfolio
Engineering	Design reviews	Standards published	Policy-as-code in CI	Signals in build & test	Agents reviewing PRs & models
Operations	Incident reviews	Runbooks & SLAs	Guardrails in runtime	Live risk scoring	Agents triaging incidents
Trust (cross-cutting)	Ethics boards	RAI policies	Bias & safety test suites	Real-time monitoring	Agentic attestation

Most enterprises are here today

Direction of travel



Operational governance evolves from manual reviews to continuous, AI-assisted governance.

SECTION 05 · OF 06

The Future

When AI governs AI — governance as an autonomous, continuous capability.

WHAT DOES AGENTIC GOVERNANCE LOOK LIKE?

Agents Help Governing AI



Humans remain accountable. AI makes governance scalable.

SECTION 06 · OF 06

The Conclusion

One framework to remember: Intent · Trust · Build · Run.

WHAT SHOULD YOU REMEMBER?

Three ideas to take with you

1

Enterprise AI has

THREE CONNECTED LIFECYCLES

2

Enterprise AI Governance connects them through

STRATEGY · TRUST · ENGINEERING · OPERATIONS

(Trust is cross-cutting)

3

The future of Enterprise AI is

AI HELPING GOVERN AI

Aligned with EU AI Act · NIST AI RMF · ISO/IEC 42001

Governance is no longer a compliance function. It is becoming an engineering capability.

Organizations that engineer **Trust** will lead the AI era.

Governance should never slow innovation. Governance should make it scalable.

THANK YOU

Let's continue the conversation

SESHU T

Associate VP

Siemens Technology India

seshubabu.tolety@siemens.com

+91 98860 52473

Governance becomes an engineering capability when intent, trust, build and run are instrumented together.

Happy to exchange notes on agentic governance, policy-as-code and AI assurance.