

Building the AI-Ready Foundation: Governance and Trust for IT Operations

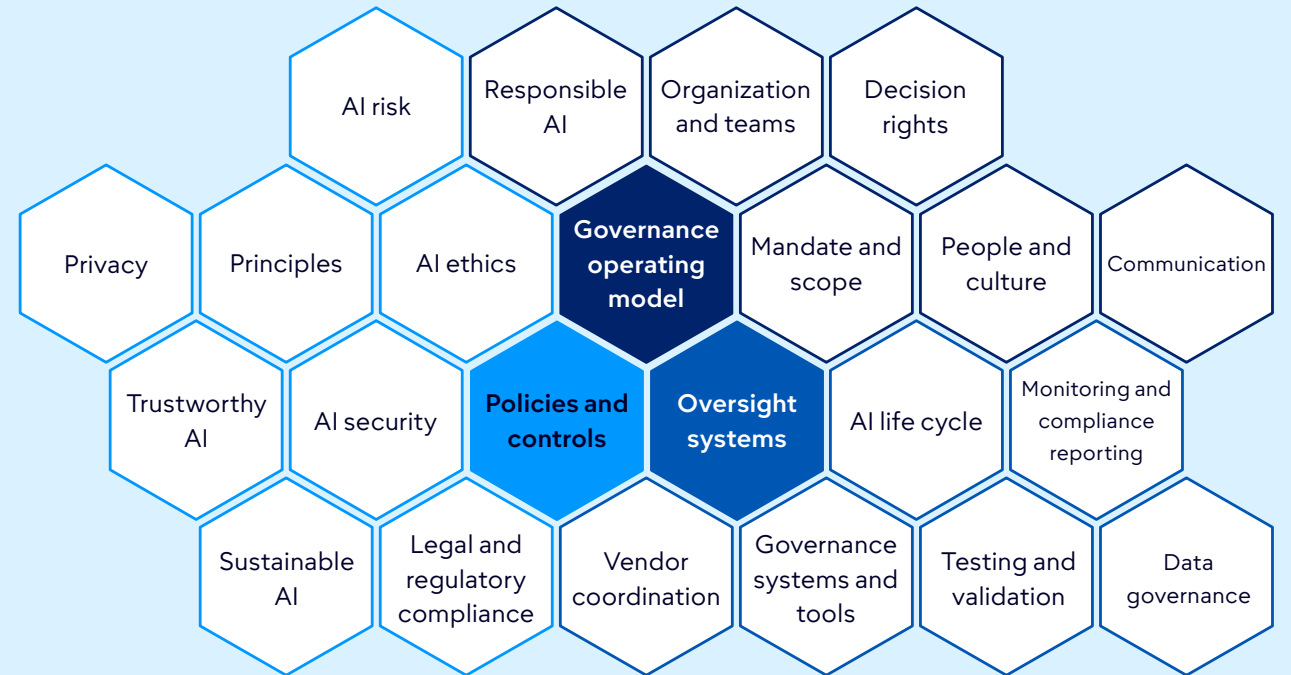


How can organizations operationalize agentic AI governance to keep pace with innovation while managing risk, regulation and trust?

As AI — especially agentic AI — rapidly scales into production, heads of infrastructure and operations (I&O) face a critical challenge: Traditional, manual approaches to controlling risk are too slow, fragmented and reactive to be effective. These legacy methods can't keep up with the speed, autonomy and complexity of modern autonomous agents, leading to unmitigated risks, compliance gaps and stalled innovation.

Without embedding automated, real-time controls into production environments, organizations risk both exposure and loss of trust. This creates an urgent need to operationalize governance — moving from static policies to dynamic, enforced controls. This roadmap equips CIOs and technology leaders with a practical path to embed and scale agentic AI governance. By aligning policies with automated controls and enabling technologies, organizations can mitigate risk, accelerate innovation and ensure autonomous agents are compliant, resilient and trusted by design.

Key components of AI governance (honeycomb)

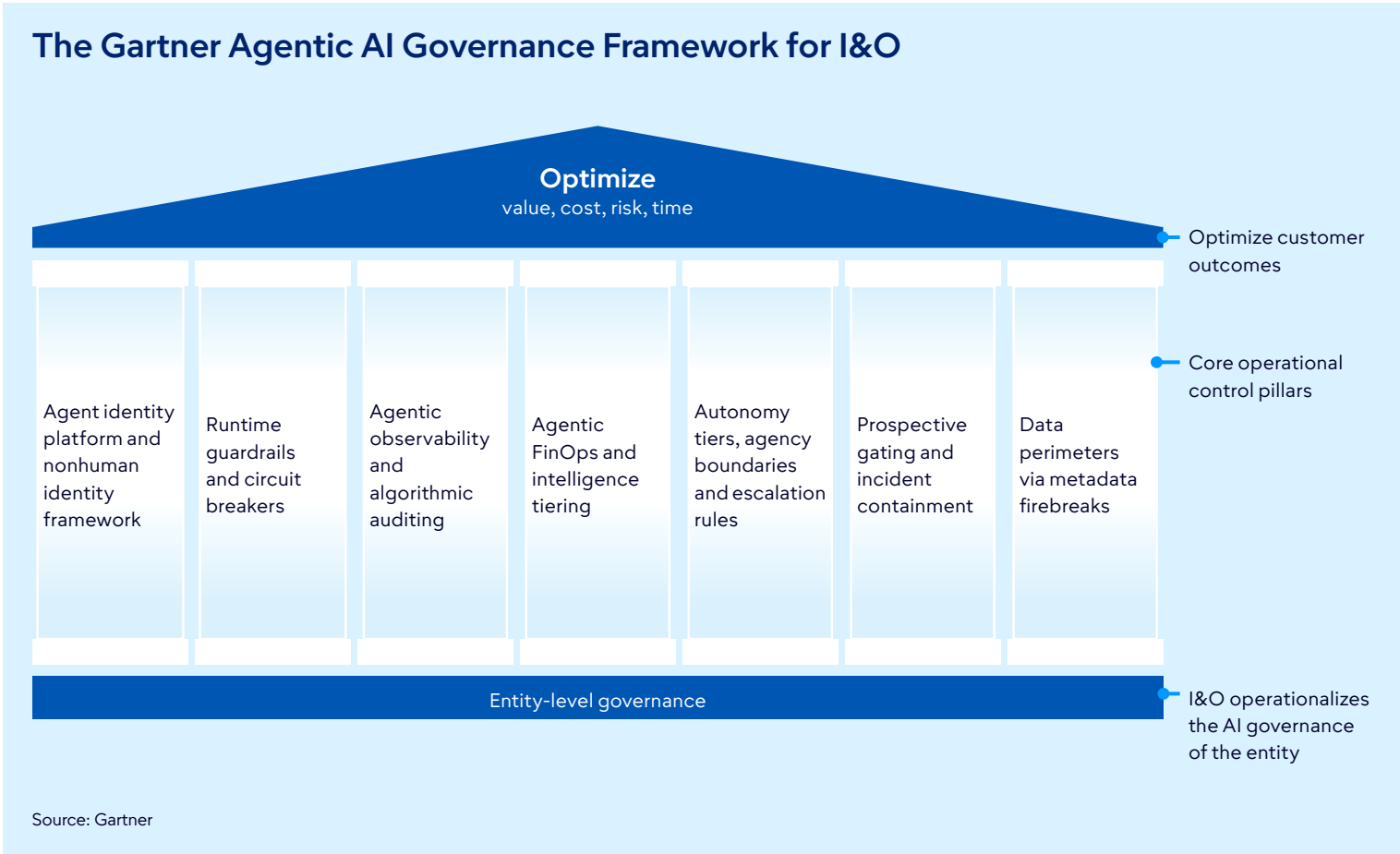


Source: Gartner

How can organizations ensure AI delivers value while meeting rising demands for transparency, security and ethical responsibility?

For heads of I&O, governing agentic AI requires the Gartner seven-pillar framework for safe, cost-effective adoption. First, establish identity by classifying all agents as nonhuman identities for total accountability. Next, implement guardrails via automated circuit breakers to prevent system runaway, and enforce FinOps using dynamic budgets to prevent financial overruns. Additionally, observability ensures compliance by continuously tracking AI reasoning chains.

To guarantee system security, escalation protocols preserve human authority over high-risk actions through strict approval gates. Containment measures, including automated kill switches, halt unauthorized actions before execution, while strict data and context perimeters protect against data exfiltration and context poisoning.



Top questions around AI governance, trust, risk and security include:

- 1

How can we align AI governance with business goals while meeting regulatory requirements?
- 2

What steps can ensure our AI systems remain ethical, transparent and secure as we scale?
- 3

How do we identify, assess and mitigate the top risks in our AI use cases and operations?

What are the key stages?

This roadmap shows the sequence of objectives and desired outcomes — a useful tool for aligning all stakeholders. It’s distilled from interactions with clients who’ve successfully implemented AI governance initiatives. A few key milestones and associated Gartner resources are highlighted below, but our full roadmap includes complete milestones and resources for each stage of governance initiatives.





Understand enterprise AI policies and define required controls

Actions to take:

- ☐ Align with enterprise AI policies and risk appetite with governance teams.
- ☐ Translate policies into concrete, implementable control and evidentiary data requirements.
- ☐ Educate stakeholders on AI risks and operational constraints.

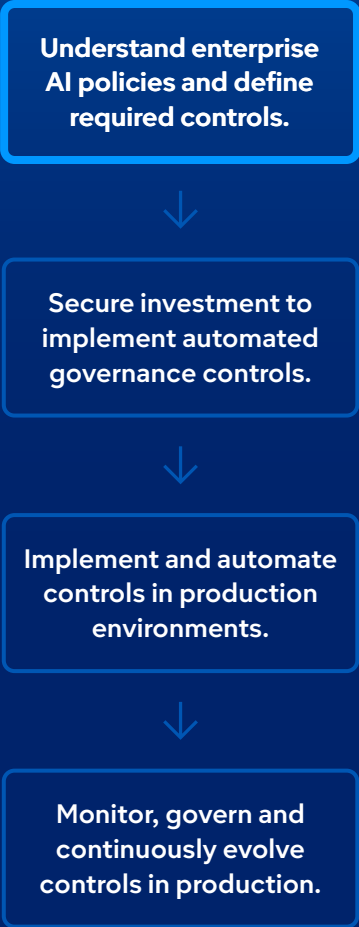
Sample of associated Gartner resources include:

- Insights**

 - Market Guide for AI Trust, Risk and Security Management
 - The Pillars of a Successful Artificial Intelligence Strategy
 - Executive AI Governance Playbook
 - The Agentic AI Governance Framework for Infrastructure and IT Operations
- Tools**

 - Policy Template for Acceptable Use of Generative AI
 - Identify and Mitigate Top GenAI Usage Risks
 - Legal and Compliance AI Use Case Risk Assessment
- Analyst Consultation**

 - How should I organize my team to enable AI governance?
 - How do we centralize governance in a distributed environment?
- ... and more





Secure investment to implement automated governance controls

Actions to take:

- ☐ Link agentic AI governance to business value and risk outcomes to secure support.
- ☐ Educate executives and the board on regulatory and compliance implications.
- ☐ Establish a cross-functional council to align priorities and investments.

Sample of associated Gartner resources include:

Insights

- Board Presentation: Resource Slides on Generative AI
- Seize the Opportunities: How Will U.S. Policy on AI Impact Business Strategy?
- Getting Ready for the EU AI Act, Phase 1: Discover and Catalog
- Data Governance and Management Investments Boost Financial Performance

Toolkit

- Building Trust to Maximize Your AI ROI

Analyst Consultation

- How do I balance innovation with control?
- How do I come up with a framework to understand risk and how it applies to AI?

... and more

Understand enterprise AI policies and define required controls.



Secure investment to implement automated governance controls.



Implement and automate controls in production environments.



Monitor, govern and continuously evolve controls in production.



Implement and automate controls in production environments

Actions to take:

- ☐ Design an AI governance operating model with clear policies and decision rights.
- ☐ Implement and automate security, risk and ethical controls.
- ☐ Assign ownership for AI systems, data and compliance.

Sample of associated Gartner resources include:

Insights

- How to Design an Effective AI Governance Operating Model
- Developing Generative AI Policy Guidance: 5 Decisions to Make
- Generative AI Adoption: Top Security Threats, Risks and Mitigations
- A Journey Guide to Successful Data and Analytics Governance
- Model Risk Controls to Implement AI Governance

Toolkits

- Template for Acceptable Use of Generative AI
- Generative AI Security Policy Template

Case Study

- An AI Governance Framework for Managing Use Case Ethics

Analyst Consultation

- How do I operationalize AI governance?
- How do I scale AI governance?

... and more

Understand enterprise AI policies and define required controls.



Secure investment to implement automated governance controls.



Implement and automate controls in production environments.



Monitor, govern and continuously evolve controls in production.



Monitor, govern and continuously evolve controls in production

Actions to take:

- ☐ Extend governance controls across new use cases and environments.
- ☐ Promote ongoing AI literacy to support responsible adoption.
- ☐ Continuously monitor, adapt and improve controls as risks evolve.

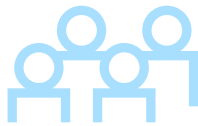
Sample of associated Gartner resources include:

- | | |
|--|--|
| Insights <ul style="list-style-type: none">• Use TRiSM to Manage AI Governance, Trust, Risk and Security• Use Model Guardrails to Regulate Generative AI Output and Behavior• Getting Ready for the EU AI Act, Phase 3: Managing Third-Party Risks• Operationalize AI Governance Post Deployment | Tools <ul style="list-style-type: none">• Documenting AI Reference Architectures• Generative AI Security Policy Template• Policy Template for Acceptable Use of Generative AI• Employee Generative AI Risk and Compliance Training Deck Analyst Consultation <ul style="list-style-type: none">• How do I monitor for risks?• How do I make people aware of the use cases for AI, risk and ROI calculations? <p>... and more</p> |
|--|--|



Who needs to be involved?

The most successful companies establish cross-functional teams to realize value from data, analytics and AI. Explore the recommended functions and roles to include for the best chance of success.



How Gartner supports your priorities

In addition to guidance on effective AI governance, Gartner also supports the priorities of CIOs, CDAOs and CISOs.

Gartner for Chief Information Officers

CIO Mission-Critical Priorities (MCPs)

Accelerate AI Enterprise Value Realization at Scale

Only 20% of AI initiatives currently deliver ROI and only 2% deliver disruptive value (Return on Future or ROF).

Manage Costs Strategically to Spend Smarter and Scale Faster

Only 18% of CIOs currently rate themselves as effective at dynamic prioritization of resources which is a significant driver of their ability to deliver business value from technology investments.

Build the Human-AI Workforce

45% more business value is driven by future-ready talent strategies, yet only 36% of CIOs are effective at building them.

Secure Growth in the Age of AI through Cybersecurity

77% of CIOs rate security and risk-related factors as top challenges to successfully implementing autonomous technologies at scale in their enterprise.

Modernize Enterprise Platforms to Enhance Agility and Performance

Only 54% (1 in 2) of CIOs rate their IT organization as effective at equipping their enterprise with the required platforms and tools needed.

Redesign IT Operating Model for Effectiveness in Turbulent Times

Only 24% of CIOs report they have been highly effective at establishing an IT operating model that flexes with changing business needs.

Architect the Next-Generation Enterprise for a Tech-Intensive Future

Only 31% of CIOs rate themselves as effective at fostering ongoing enterprise-wide, technology-enabled innovation.

With Gartner for CIOs, you can confidently navigate complex technological environments, make smarter decisions and deliver stronger results. Our insights, guidance and tools are designed to focus specifically on the mission-critical priorities of CIOs and their teams.

Whether you’re looking to unlock better value with AI, optimize costs or lead organizational change, Gartner for CIOs can help you act fast and demonstrate value – from strategy to execution.

Gartner for Infrastructure & IT Operations Leaders

Head of Infrastructure & IT Ops Mission-Critical Priorities (MCPs)

Transform Cloud Strategy for Disruptive Platform Demands

By 2030, companies that fail to optimize the underlying AI compute environment will pay over 50% more than those that do.

Change the Conversation on Technical Debt Management

Accumulation of Technical Debt is the top challenge for Heads of I&O - 44% rate it as one of their top 3 challenges.

Reinvent I&O as an Enabler of AI Value

77% of CEOs say AI is ushering in a new business era rather than introducing a new technology.

Gartner for Infrastructure & IT Operations Leaders helps heads of I&O and their teams make stronger, faster decisions. Our insights, guidance and tools focus on the mission-critical priorities that matter most to your organization and stakeholders.

From enabling AI value and modernizing cloud strategy to managing technical debt and optimizing operations, Gartner empowers I&O leaders with actionable insights, expert guidance and proven tools to drive business value, mitigate risk and improve efficiency.

Gartner for Chief Information Security Officers

CISO Mission-Critical Priorities (MCPs)

Build and Evolve a Resilient and Agile Cybersecurity Program

Only 14% of Non-Executive Directors are very or extremely confident in the effectiveness of current cyber risk assessments.

Adapt Cybersecurity Strategies for AI

91% of senior business leaders see AI as a value driver, making AI cybersecurity governance essential.

Optimize Cybersecurity Technology and Architecture Effectiveness

75% CISOs identify budget or resource constraints as a challenge to meet their strategic objectives in the next 6 months.

Gartner for CISOs delivers insights, guidance and tools designed to directly address today’s complex cybersecurity challenges and the imperatives that matter most to your stakeholders.

As the CISO role moves closer to the front lines of strategic influence, Gartner supports leadership effectiveness with data-driven cybersecurity coverage on your top priorities, including protection level agreements, third- and fourth-party risk, talent management, AI governance and more.

360-degree coverage for heads of I&O and their teams

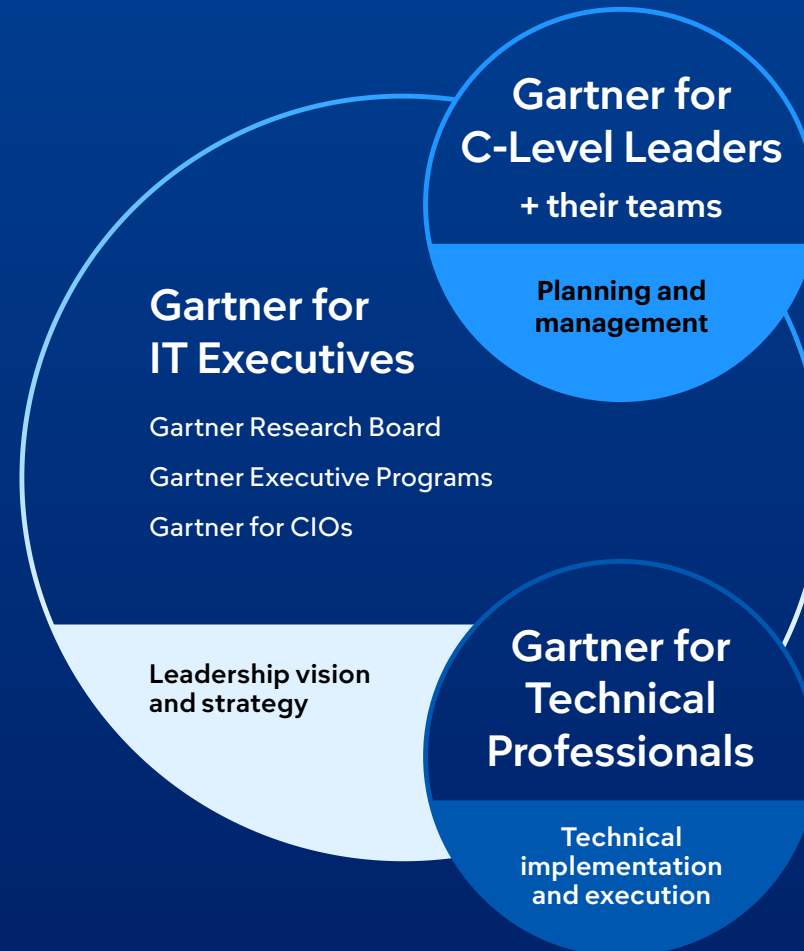
Expert guidance and tools to maximize
success at every level

Validate your vision and empower teams to execute with confidence.

Heads of I&O rely on Gartner for Technical Professionals (GTP) to kick-start their most crucial projects. Instead of starting from scratch, they tap into expert resources to help accelerate their teams' performance. GTP offers purpose-built tools, proven technical plans, assessments, models, step-by-step guides, reference architectures and roadmaps — all designed to help you achieve better business outcomes when you engage as a team.



Get access to technical analysts and role-specific
peer communities with GTP.



CISO/security and risk leaders
CDAO/data and analytics leaders
Software engineering leaders
Heads of infrastructure and
IT operations
Enterprise IT leaders

Data and AI architects
Infrastructure and cloud architects
Software and applications architects
Security architects

Gartner

Actionable, decision intelligence

Explore these additional complimentary resources and tools on AI governance for data and analytics leaders:

Roadmap



3 Key Trends Shaping the I&O Landscape

Learn how I&O leaders are aligning strategy, reducing risk and accelerating AI-driven infrastructure transformation.

[Download Now](#)

Webinar



Avoid 3 Key Mistakes in Technical Debt Management

Learn how leading organizations are avoiding technical debt pitfalls with stronger governance, accountability and risk-based decision making.

[Watch Now](#)

Webinar



How to Use Generative AI in Cloud Operations

Learn how cloud operations leaders are prioritizing high-value GenAI use cases to drive measurable business outcomes at scale.

[Listen Now](#)

Conference



Gartner IT Infrastructure, Operations & Cloud Strategies Conference

Save the date to discover the latest I&O strategies and connect with industry peers.

[Learn more](#)

Already a client? Get access to even more resources in your client portal. [Log In](#) ↗

Connect with us

Get actionable, objective decision intelligence to deliver on your mission-critical priorities. Our expert guidance and tools enable faster, smarter decisions and stronger performance. Contact us to become a client:

U.S.: 1 855 322 5484

International: +44 (0) 3300 296 946

Become a Client

Learn more about Gartner for IT Leaders
gartner.com/industries/information-technology

Stay connected to the latest insights

