Bigeye

AI Trust Assessment Results

Operational Stage

Your organization has achieved what most aspire to.

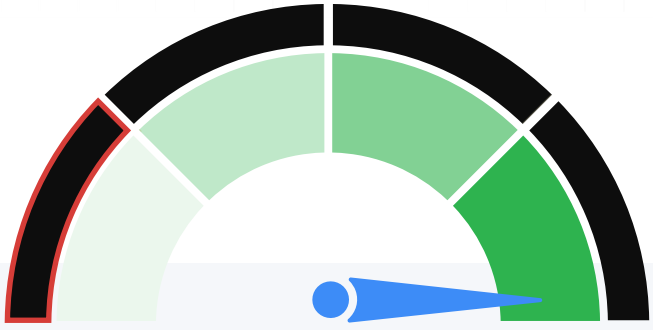
What is AI Trust?

Most traditional data tools assume a human is thoughtfully deciding what data to access. AI agents operate differently — they can access vast amounts of data very quickly, combine it in unexpected ways, and make decisions about how to use it, at machine speed.

Without AI Trust infrastructure, you can't answer fundamental questions about your AI data usage:

- What data is this agent actually using?
- What sensitive data does the agent have access to?
- What decisions are being made by the agent using this data?

AI Trust means having visibility, accountability and control over how AI agents access and use your enterprise data, and ensuring that data meets quality standards for automated decision-making.



Introducing the
AI Trust Maturity Scale

To build and deploy AI responsibly you need a foundation of trust in the data that powers them. The AI Trust Maturity Scale helps teams understand where they stand today, and what it will take to move forward with confidence.

This scale isn't about theoretical best practices. It's about the real, operational steps that determine whether your AI initiatives can succeed and how much risk you're taking on along the way.

Your score reflects your team's current position on that scale. From there, you can begin identifying the biggest gaps, mapping realistic next steps, and building the infrastructure to support AI you can trust.

The Five Stages of AI Trust Maturity

Here's how the five maturity stages break down, from most mature to least mature.

Operational

You've built scalable guardrails around AI data usage with comprehensive oversight frameworks. Agents' data access are monitored and controlled with systematic rigor. Data quality, sensitivity classifications, and certification status are tracked and enforced automatically. AI decisions are auditable, and safe to scale.

Ideal business outcomes: AI initiatives launch faster with continuous governance. Scaling decisions are data-driven rather than risk-averse.

Success indicators: AI agents are automatically blocked from accessing unauthorized datasets before decisions are made, with real-time policy enforcement that validates every data request against sensitivity classifications and usage policies. Audit trails capture not just what data was used, but what agents attempted to access, including blocked requests and policy violations. When data classification or access rules change, updates are enforced across all AI systems, ensuring no unauthorized access incidents happen and. Teams are confident that agents operate only within their approved scope.

Managed (YOU ARE HERE)

You've implemented structured data classification, quality monitoring, and approval processes across much of your data. Teams understand which data is validated for AI use, and consistent controls are in place to guide agent behavior.

Ideal business outcomes: Security and legal teams approve AI projects with confidence. Data-related incidents are rare and quickly resolved.

Success indicators: New AI use cases can be evaluated systematically against established data governance frameworks, with clear approval workflows that security and legal teams trust. When agents attempt to access data outside their approved scope, controls are in place to flag or restrict the action before inappropriate usage occurs. Data quality issues that could impact AI decisions are identified and resolved within defined SLAs, and teams can quickly determine whether specific datasets meet the standards required for AI consumption across different use cases.

Emerging

You've built some of the necessary foundations: creating inventories, defining data characteristics, and introducing light controls around quality and usage. You're gaining visibility into your AI data landscape, but oversight is still limited and coverage is incomplete.

Ideal business outcomes: AI pilots move to production with fewer data-related surprises because teams have visibility into which datasets have been characterized and validated. Basic data controls can be demonstrated to stakeholders when questions arise about AI data usage.

Success indicators: Teams can identify gaps in coverage before they become blockers. Data inventories provide enough foundation to make informed decisions about which datasets are appropriate for specific AI use cases, even if comprehensive automation isn't yet in place.

Aware

You've recognized the need for oversight, but efforts are informal or inconsistent. Data stakeholders may be flagging risks manually, and there's growing concern about how data is used in AI, but no shared system to manage it systematically.

Ideal business outcomes: AI initiatives proceed with cautious optimism rather than fear. Internal teams understand and can articulate data-related risks.

Success indicators: Data issues are identified and discussed, even if resolution is inconsistent. Cross-functional teams collaborate on AI data concerns.

Unaware

You don't have many, if any, structured processes in place for data preparation, validation, or approval for AI use. Your organization may not even be aware of what's missing or understand the right steps to take. This is essentially "stage 0" -- where every organization starts, with no structure around AI data management.

Ideal business outcomes: AI experiments begin, though scaling is blocked by unknown risks and stakeholder concerns.

Success indicators: The organization recognizes that data governance matters for AI success.

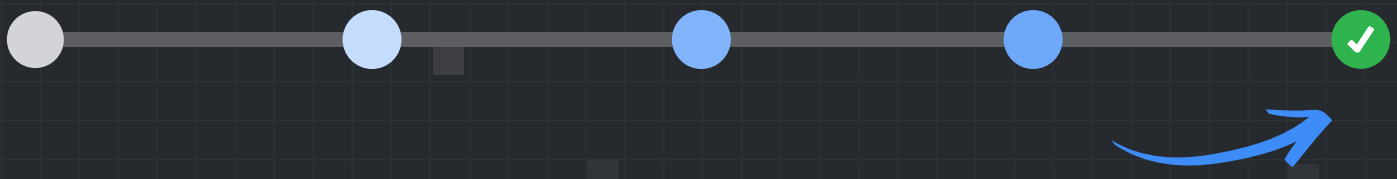
What your score means

You're in the Operational stage of AI trust maturity.

At this stage, your organization has achieved what most aspire to: comprehensive, automated AI data governance that operates at machine speed. You run formal cross-functional governance programs with active stakeholder engagement and decision-making authority. Your data governance structure integrates clearly defined roles and responsibilities across business, data, and technology teams with regular engagement.

Your quality management is fully automated organization-wide, measuring and monitoring key data quality dimensions across all critical datasets with thresholds and alerts tied to business impact. You have automated detection for both in-flight and at-rest data issues, and you track resolution metrics to continuously improve processes and team performance. Your classification systems are automated and policy-driven, with enforcement tied to data use and access.

You've already achieved end-to-end observability with automated alerts, impact analysis, and trust indicators tied to pipeline performance. Your AI governance program is well-established and drives policy, risk management, ethical standards, and cross-functional accountability. AI-ready data is clearly marked, easily discoverable, and tied to comprehensive quality, privacy, and governance metadata.



What this enables for your organization

Your operational maturity unlocks capabilities that create significant competitive advantages:

Innovation velocity

Your automated governance processes enable rapid AI experimentation and deployment. New use cases can be evaluated, approved, and deployed quickly because validation happens automatically. Teams can innovate without waiting for manual approval cycles or worrying about compliance gaps.

Regulatory confidence

Your comprehensive audit trails, automated lineage tracking, and integrated compliance processes mean regulatory inquiries are handled in hours rather than weeks. You can confidently enter regulated markets and pursue AI applications that less mature organizations cannot.

Strategic scaling

Your end-to-end observability and automated governance mean scaling decisions are data-driven rather than risk-averse. You can expand AI usage across the organization systematically, knowing your trust infrastructure will maintain governance at any scale.

Competitive positioning

While competitors struggle with basic data governance, you can focus resources on AI innovation and strategic advantage. Your operational maturity becomes a business differentiator that compounds over time.

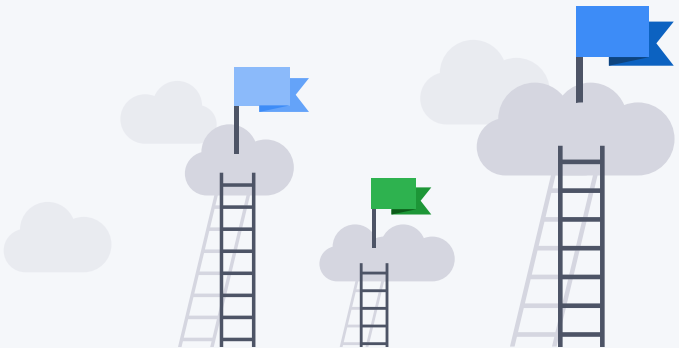
How the most mature orgs are operating

Organizations building AI trust into their infrastructure are moving beyond visibility. They're implementing enforceable controls that align to real business and compliance risk — without slowing down delivery.

Capability	Unaware	Aware	Emerging	Managed	Operational
Data Visibility	No or little visibility into AI data usage	Awareness of what data sources AI has access to	Systematic inventory of AI data sources	Comprehensive data cataloging with ownership	Real time monitoring of what data is being accessed by AI
Data Controls	No or little restrictions on AI data access	Informal guidelines for data use	Light controls and basic approval processes	Structured policies with consistent enforcement	Automated guardrails with real-time enforcement
Quality Management	Quality issues generally discovered after problems occur	Manual quality checks intermittently	Regular quality monitoring for key datasets	Systematic quality validation processes	Continuous quality assurance integrated into workflows
Risk Assessment	Unaware of full scope of data-related AI risks	Recognizes risks but no systematic approach	Basic risk identification and documentation	Structured risk management with regular reviews	Comprehensive risk monitoring with automated alerts

The Complete Journey to AI Trust Maturity

To reach full operational maturity, organizations need to build capabilities across three core areas. Here's how they connect:



Quality Foundation: Know Your Data

Start by understanding what data your AI systems use and whether it's appropriate:

- **Map your AI data landscape** - Catalog which datasets, tables, and columns your AI systems access
- **Set usage boundaries** - Define which data fields should and shouldn't be available for AI consumption
- **Monitor data health** - Implement tracking for completeness, accuracy, timeliness, and consistency
- **Define fitness criteria** - Document what makes data appropriate for your specific AI use cases and create workflows to validate readiness
- **Handle problem data** - Build processes to identify and quarantine data that isn't ready for AI use

Sensitivity Controls: Protect What Matters

Control how sensitive information flows through AI systems:

- **Create approved inventories** - Maintain clear lists of datasets authorized for AI access
- **Classify for sharing** - Categorize all AI data by sharing permissions (Public, Internal, Confidential, Restricted)
- **Tag sensitive content** - Identify and mark PII, PCI, PHI, and other sensitive data types at the column level
- **Track privacy risks** - Maintain ongoing logs of privacy concerns and establish policies for sensitive data handling (like requiring SSN hashing)

Certification Framework: Validate and Approve

Ensure data meets all requirements before AI systems use it:

- **Combine quality and privacy assessments** - Document whether datasets meet both technical and sensitivity standards
- **Formalize approval workflows** - Create structured processes to validate and authorize data for AI use
- **Establish oversight** - Implement management processes aligned with industry standards for quality, security, and risk management
- **Maintain governance alignment** - Ensure practices meet established data management frameworks

The key insight: These concepts build on each other as you get more mature in your approach to AI ready data. You can't properly classify data until you know what you have, and you can't certify data until you understand both its quality and sensitivity profile.

Your Immediate Focus: Maintaining Operational Excellence

While you've achieved the highest level of AI trust maturity, the landscape continues evolving. Your focus should be on maintaining excellence while staying ahead of emerging challenges:

Evolving AI Capabilities

- **Monitor emerging AI technologies**
  As new AI capabilities emerge (multimodal models, agent frameworks, etc.), ensure your processes adapt to handle new data types and usage patterns
- **Expand automated coverage**
  Continuously extend to cover new data sources, AI applications, and business processes as they emerge

Regulatory Evolution

- **Stay ahead of compliance requirements**
  Leverage your automated audit capabilities to prepare for evolving regulations before they take effect
- **Influence standards development**
  Organizations at your maturity level often participate in industry standards development and best practice sharing

Organizational Leadership

- **Share best practices**
  Your operational maturity positions you to influence industry approaches to AI Trust
- **Mentor other organizations**
  Consider thought leadership opportunities to help advance the broader ecosystem

Continuous Optimization

- **Refine automated processes**
  Use your resolution metrics and trend reporting to continuously optimize AI Trust processes
- **Expand business value measurement**
  Move beyond risk mitigation to measure how AI trust infrastructure drives business value

Why it matters now

Your operational maturity becomes increasingly valuable as the AI landscape accelerates. Several trends make your position particularly advantageous:

AI governance complexity is increasing

As AI capabilities expand, governance requirements become more sophisticated. Your automated, comprehensive approach positions you to handle this complexity.

Regulatory scrutiny is intensifying

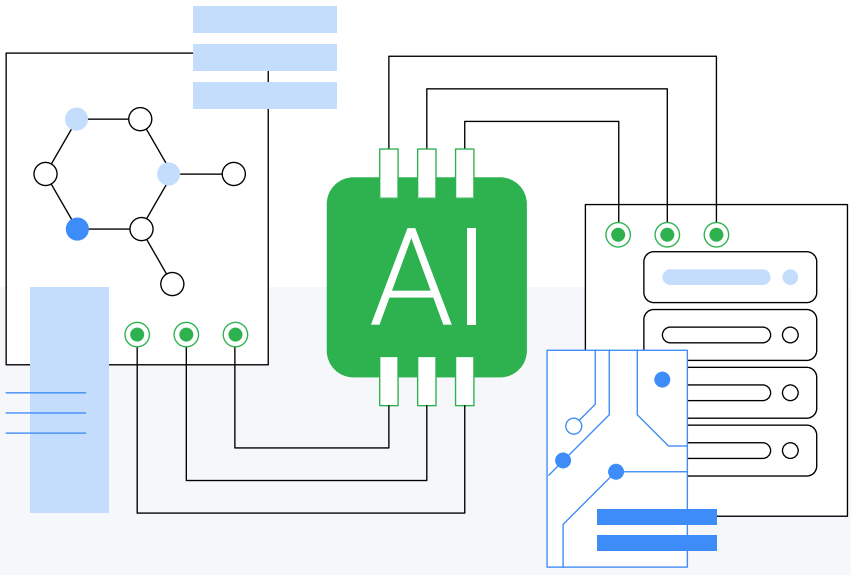
Global AI regulations are expanding rapidly. Your automated compliance capabilities and comprehensive audit trails position you to navigate regulatory complexity that will overwhelm less mature organizations.

Competitive differentiation through trust

As AI becomes ubiquitous, trust becomes a differentiator. Organizations that can demonstrate comprehensive AI governance gain competitive advantages in customer confidence, partnership opportunities, and market access.

Your operational maturity isn't just about managing current AI initiatives, it's the foundation that enables you to pursue AI strategies others cannot, respond to regulatory changes quickly, and scale at speeds others cannot match.

The organizations that maintain and evolve operational excellence become industry leaders not just in AI capability, but in responsible AI deployment that creates lasting competitive advantage.



What to do next

Looking for an AI Trust platform to add to your stack?

Talk to our team

Bigeye