TrustCloud®

CISOs' Guide to AI Governance

How the world's Security Leaders are balancing AI Innovation with their Core Responsibility to Protect Their Organizations from Risks

TABLE OF CONTENTS

3 **Introduction** Why AI Governance Matters

5 **Chapter 1.** Corporate AI Governance: Defining Your AI Strategy

7 **Chapter 2.** Managing Internal AI Risk: First-Party AI Governance

8 **Chapter 3.** Managing External AI Risk: Third-Party AI Governance

9 **Chapter 4.** AI Regulations and Compliance

10 **Chapter 5.** AI Governance and Ethics

13 **Conclusion**

14 **Further Reading and Resources**

INTRODUCTION:
WHY AI GOVERNANCE MATTERS

AI is spreading fast, and with it, pressure is mounting on CISOs. As enterprises race to deploy artificial intelligence, CISOs and security leaders are now asked to perform a delicate balancing act: drive innovation forward without compromising security, privacy, or compliance.

With AI comes the promise of operational transformation—boosting efficiency, unlocking insights, and accelerating product development. But this promise comes with high-stakes risks: opaque decision-making, exposure of sensitive data, compliance gaps, and growing scrutiny from regulators and customers.

“The urgency is real. CISOs are expected to move quickly, but with care. The challenge is implementing an AI governance framework that allows your business to innovate confidently while minimizing risks.”

Sravish Sridhar
CEO of TrustCloud

This guide explores how to achieve that balance, offering a comprehensive approach to AI governance with real-world examples and practical steps.

THE CORPORATE AI GOVERNANCE FRAMEWORK

An effective AI governance strategy addresses **five key areas:**

- **AI Governance Foundation & Alignment:** Establishing policies, accountability, and an AI governance committee.
- **Internal (First-Party) AI Risk:** Managing AI tools, employee usage, and assessing AI risk within the organization.
- **External (Third-Party) AI Risk:** Evaluating vendor AI risk and contractual safeguards.
- **AI Regulations and Compliance:** Aligning with standards such as NIST AI RMF and ISO 42001 and ensuring compliance with applicable regulations.
- **Customer Assurance:** Addressing concerns about AI's impact on data security and privacy, and providing clear, standardized responses to AI-related security questions.

Internal (first-party) AI risk

What is the list of approved AI tools and technologies? For what purposes?
How do we ensure that employees are not using public AI?
What is the process for requesting new tools? Who approves?
Do we develop AI models? How are we assessing risk in our models?
Do we have an AI risk register?

AI Regulations and Compliance

What AI regulations apply to us? How do we keep up with new ones?
Should we align to a standard like NIST and ISO 42001? What will it take?
Are any customers asking for compliance?

Corporate AI Governance

How do we balance enabling innovation vs. limiting our AI risk?
What is the organization's overarching policy about AI usage?
Who is responsible for what? Legal / CISO / Department leaders?
How do we create an AI governance committee and who should be on it?

External (third-party) AI risk

How are we assessing our vendors for AI in their products?
What are acceptable answers from vendors? What gets flagged?
What contractual terms needs to be added to protect our data?

Customer Assurance

Are customers asking questions about our use of AI (as it pertains to customer data)
How are we answering today? What's the right way to answer to avoid additional scrutiny? What material do we need to create?

“The first step in establishing an AI governance program is figuring out who is responsible for what actions. This might include top management sponsors, compliance program managers, regulatory and legal compliance advisors, risk owners, as well as technical SMEs. From there, it is a matter of aligning with, or assessing against, one of the common risk management frameworks, such as the NIST AI RMF.”

David Forman
Founder, Mastermind Assurance

CHAPTER 1:
CORPORATE AI GOVERNANCE: DEFINING YOUR AI STRATEGY

❓ Key Questions

- **How do we balance enabling innovation vs. limiting AI risk?**
- **What is our overarching AI policy?**
- **Who is responsible for AI governance, and what roles do different functions play (Legal, CISO, Department Heads)?**
- **How do we form and operate an AI governance committee?**

👍 Best Practices

- **Establish a Cross-Functional AI Governance Committee:** Bring together leaders from legal, compliance, IT, engineering, and security. This group should align on guiding principles, assign ownership, and set a meeting cadence to ensure progress and accountability.
- **Develop and Enforce an AI Usage Policy:** Define the appropriate and prohibited uses of AI within your organization. This includes language models, machine learning tools, and automated decision-making systems. Your policy should reflect your risk tolerance, compliance requirements, and ethical commitments.
- **Monitor and Audit AI Usage:** Establish controls to log and review how AI is being used, particularly in sensitive business functions. Regular internal audits can surface unintended usage or compliance gaps before external regulators or customers do.

"Every organization needs a structured AI governance philosophy. CISOs & Security leaders must balance being enablers and even drivers of innovation while maintaining their core responsibility of securing and protecting the organization from threats. You have to do both to stay competitive."

Tejas Ranade
Chief Product Officer of TrustCloud

CHAPTER 2:
MANAGING INTERNAL AI RISK: FIRST-PARTY AI GOVERNANCE

❓ Key Questions

- What is our risk tolerance?
- How is AI used in our products and services?
- What AI tools and technologies are approved for internal use?
- How do we prevent employees from using unauthorized AI tools?
- Do we maintain an AI risk register?

👍 Key Questions

- **Create a Formal AI Tool Approval Process:** Standardize how AI tools are evaluated and approved, including legal, security, and data protection reviews before adoption.
- **Implement Employee Training:** Provide mandatory training for staff on acceptable AI use, data handling risks, and scenarios to avoid (e.g., inputting sensitive data into public LLMs).
- **Conduct and Document AI Risk Assessments:** Run structured assessments of each AI initiative. Evaluate its purpose, data sources, potential bias, and security vulnerabilities.
- **Establish Internal AI Controls:** Implement controls to manage model drift, unauthorized use, and over-dependence on automation. Review controls regularly as usage evolves.

“The biggest challenge organizations face is not knowing where to start. A strong AI governance framework needs clear policies, risk assessments, and visibility into AI usage.”

Tejas Ranade
Chief Product Officer of TrustCloud

CHAPTER 3:
MANAGING EXTERNAL AI RISK: THIRD-PARTY AI GOVERNANCE

Key Questions

- How do we assess AI risk in vendor products?
- What contractual terms should be included to protect our data?
- What are acceptable answers from vendors regarding AI governance?

Key Questions

- **Conduct Structured AI Vendor Risk Assessments:** Incorporate AI-specific questions into your third-party risk assessment process. Ask about their use of AI, training data, model governance, and auditability.

- **Include AI-Specific Contractual Terms:** Require vendors to disclose AI use, agree to data protection clauses, and submit to audit rights. Align terms with your internal AI usage policy.

- **Monitor Vendor Compliance:** Establish a system for ongoing risk evaluation. If a vendor updates its AI models or launches new features, re-evaluate risk based on their changes.

"Many organizations overlook third-party AI risk. Having a structured approach to vendor management is what will make your compliance and data security make or break — and frankly, what's needed to keep up with how fast AI is moving."

Tejas Ranade
Chief Product Officer of TrustCloud

CHAPTER 4:
AI REGULATIONS AND COMPLIANCE

Key Questions

- What AI regulations apply to our organization?
- How do we align with frameworks like NIST AI RMF and ISO 42001?
- Are customers asking for AI standards compliance?

Best Practices

- **Map Governance to NIST AI RMF and ISO 42001:** Start with these emerging global frameworks to build structure into your policies and documentation. Tailor their guidance to your specific context.
- **Implement Continuous Compliance Monitoring:** Use automation where possible to track compliance metrics, update documentation, and generate audit logs in real time.
- **Engage Customers Through Transparency:** Be proactive. Share how you govern AI with prospective customers. Use trust portals to publish summaries of controls, certifications, and assessments.

Industry Trend

According to a 2024 Gartner report, over **60% of enterprises** will require formal AI governance frameworks by **2026** to meet rising security, risk, and compliance demands.

CHAPTER 5:
AI GOVERNANCE AND ETHICS

AI governance is not complete without a strong ethical foundation. Ethical considerations must be baked into how AI is designed, trained, and deployed across the organization. It's not only about regulatory compliance, but about public trust and long-term sustainability.

Ethical Best Practices:

- **Align AI Use with Organizational Values:** Review AI decisions for fairness, accountability, and transparency. Document decisions that impact people, customers, and communities.
- **Establish an AI Ethics Review Process:** Include stakeholders from diverse backgrounds to evaluate high-risk use cases.
- **Ensure Human Oversight:** Avoid black-box AI systems. Require review and override mechanisms for any automated decisions with material impact.

For deeper perspective on this topic, read: Balancing Innovation and Ethics: Navigating Data Privacy in AI Development

> *"Given our strong relationship with TrustCloud and prior success achieving multiple standards, we knew their platform would be the best way to achieve the ISO 42001 certification."*
>
> Andrew Josephides
> Sr Director of Infrastructure and Security at Evisort

Real-World Examples: AI Governance in Action

- **IMO Health:** Adopted a structured AI risk assessment framework and streamlined compliance with healthcare AI regulations.
- **Cribl:** Strengthened its third-party AI risk management and emphasized the need for governance to keep innovation moving without compromising security.
- **BlueCat Networks:** Aligned its governance with NIST and ISO standards, driven by an AI governance committee.
- **Evisort:** Became one of the first ISO 42001-certified companies using TrustCloud.

Real-World Examples: AI Governance in Action

"Evisort was well-prepared to be among the first companies worldwide to receive an accredited ISO 42001 certification... TrustCloud's technology was utilized by both the Evisort and Schellman teams to drive an efficient audit process from start to finish."

Danny Manimbo
Schellman Principal and AI Assessment Leader

- **Risk Reduction:** Minimizes legal and security threats.
- **Regulatory Compliance:** Ensures readiness for evolving standards.
- **Operational Efficiency:** Automates compliance and risk assessments.
- **Customer Trust:** Demonstrates AI integrity and transparency.

“An AI governance program mitigates risk and saves countless hours spent answering customer inquiries about AI security and compliance.”

Tejas Ranade
Chief Product Officer of TrustCloud

Next Steps: Building Your AI Governance Program

1. **Establish an AI Governance Committee: I**dentify cross-functional leaders who will champion governance practices and drive adoption. Assign ownership for implementation.

2. **Create a Comprehensive Governance Framework:** Develop policies, controls, and escalation procedures aligned to your business model and risk appetite.

3. **Automate Risk and Compliance Monitoring:** Implement tools that can continuously monitor controls, identify drift, and support audit preparation.

4. **Train Employees and Vendors:** Run recurring awareness programs and workshops that help both internal teams and external partners understand your AI policies and standards.

5. **Continuously Evolve Based on Risk and Regulation Changes:** Stay up to date with AI-related laws, customer expectations, and innovation trends. Revisit your governance model quarterly.

CONCLUSION

As AI accelerates across industries, CISOs are now on the frontlines of balancing innovation with protection. This guide outlines the essential building blocks of AI governance, from foundational policy setting and internal risk controls to third-party oversight, regulatory alignment, and ethical transparency.

The message is clear: governance is no longer optional. With scrutiny from regulators, rising demands from enterprise customers, and the growing complexity of AI systems, security leaders need a structured approach that scales with the speed of innovation.

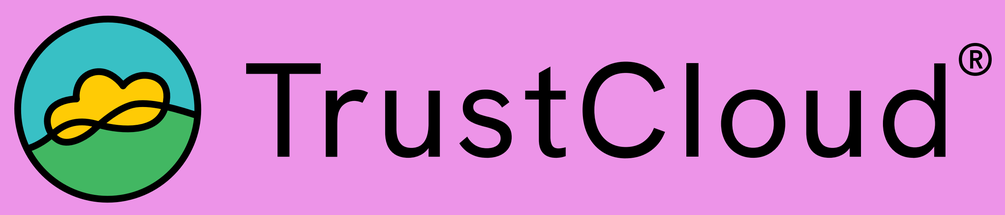
Those who get it right won't just meet compliance expectations—they'll earn trust, reduce operational drag, and enable their organizations to move faster and smarter with AI.

Organizations including Evisort, IMO Health, Cribl, and BlueCat Networks rely on TrustCloud to implement AI governance at scale.

To learn more about how TrustCloud helps CISOs build an AI governance program that scales innovation without sacrificing security, visit: TrustCloud's AI Governance Solution

FURTHER READING & RESOURCES

- [TrustCloud & Evisort Blog on Responsible AI]
- [Balancing Innovation and Ethics: Navigating Data Privacy in AI Development]
- [NIST AI Risk Management Framework]
- [ISO 42001 AI Governance Standard]



💛 Joyfully Crafted to Elevate Security and GRC Leaders into Trust Champions.