
PERSPECTIVES

AI AS IP™ FRAMEWORK:
REASONABLE MEASURES IN THE AGE
OF ARTIFICIAL INTELLIGENCE



Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

Copyright © 2026 J.S. Held LLC, All rights reserved.

Corporate Chief Intellectual Property Officers, General Counsel, and Chief IP Counsel should read this article to:

- Understand how “reasonable measures” in trade secret, patent, and copyright contexts are evolving as AI systems create, store, modify, and expose valuable intellectual property across technical and organizational layers
- Advise clients to build AI Asset Registers that document asset names, ownership status, responsible business unit, development history, deployment status, licensing restrictions, applicable protections, valuation, and governance controls
- Use governance records, including approvals, usage logs, version histories, validation reports, audit findings, access records, training records, incident reports, and policy acknowledgments, as future evidence in disputes, investigations, transactions, or insurance claims
- Identify disclosure risks arising from employee use of AI platforms and advise on approved-use policies, platform classification, escalation controls, and documentation protocols
- Anticipate litigation and transaction needs by preserving records of model versions, training data, prompt libraries, agent instructions, governance policies, audits, risk assessments, telemetry, and incident reports

Outside counsel, including law firm IP partners, technology transactions attorneys, AI governance counsel, and litigation partners advising clients on AI matters, should read this article to:

- Recognize AI as enterprise capital that can be identified, controlled, measured, licensed, transferred, monetized, and tied to revenue, efficiency, competitive

EXPERT VOICES

James E. Malackowski



In this article, AI as IP™, intellectual property valuation, AI governance, AI disputes, and intangible-asset economics expert James E. Malackowski explains how organizations can treat AI systems as protectable enterprise assets and demonstrate reasonable measures through governance, documentation, evidence preservation, and independent assurance.

Joel E. Lutzker



In this article, Joel E. Lutzker, whose expertise spans patent litigation, IP transactions, licensing, patent acquisitions, financial services IP, and international IP matters, applies decades of legal and transactional IP experience to the governance, documentation, disclosure control, and evidentiary implications of AI as intellectual property.

differentiation, and enterprise value

- Treat AI governance as an enterprise-stewardship issue requiring operational governance, management oversight, and board accountability rather than a purely technical function
- Prepare for heightened Physical AI risk by documenting testing procedures, validation activity, operational design domains, human oversight, model change control, telemetry, and incident-response readiness
- Reduce AI-washing exposure by ensuring public claims about AI capability, governance, or performance are supported by inventories, validation records, audits, governance policies, and evidence-preservation protocols
- Use AI governance ratings or independent assurance to support board oversight, investor diligence, insurance underwriting, strategic transactions, and enterprise risk management

Executive Summary

For decades, intellectual property protection has relied on a practical idea: valuable assets deserve reasonable measures. Trade secret law asks whether secrecy efforts were reasonable under the circumstances. Patent practice depends on disciplined invention records and filing decisions. Copyright protection benefits from records that show authorship, ownership, and creative contribution. These practices developed before organizations began using artificial intelligence systems to create, manage, and deploy intellectual property at scale.

In this fourth article in the AI as IP™ series, we discuss how artificial intelligence is changing the business environment. A single AI system may contain training data, model assets, algorithms, infrastructure, deployed applications, prompts, retrieval systems, agent frameworks, and governance processes. Many of these components carry independent economic value. Many also create risk when they are poorly documented or exposed to systems outside the organization's control.^{1,3}

This article argues that reasonable measures in the AI era require more than traditional confidentiality agreements or filing procedures. As AI is increasingly treated as intellectual property, new approaches are needed to protect AI assets, preserve related IP rights, and establish governance evidence through independent assurance. Organizations increasingly need AI asset inventories, disclosure controls, governance records, evidence preservation, board oversight, and independent assurance. The rise of physical AI sharpens the point. When AI operates in the physical world, failure can result in property damage, bodily injury, business interruption, insurance claims, regulatory investigations, and litigation.⁴

Introduction: The Next Stage of AI as Intellectual Property

Artificial intelligence has become one of the most significant categories of enterprise assets in the modern economy. Organizations devote substantial resources to creating, acquiring, managing, and deploying AI systems, and those systems now shape research and development, product design, software creation, customer interactions, operational decisions, and strategy. AI is no longer merely a tool that organizations use; it has become a valuable business asset.^{1,2}

The earlier articles in the AI as Intellectual Property, or AI as IP™ series, traced this shift. The first argued that AI systems should be treated as recognizable forms of intellectual property that can be protected, valued, licensed, and monetized through established frameworks. The second extended the analysis to boards, executives, and investors, proposing that AI assets represent a form of enterprise capital requiring governance, valuation, and stewardship comparable to other major corporate assets. The third applied these ideas to small and medium-sized enterprises, offering a practical framework for identifying, protecting, and commercializing AI-related assets.^{1,2,3}

A question follows naturally. If AI assets are intellectual property, what constitutes reasonable measures for their protection?

Intellectual property law generally does not require absolutes. Trade secret owners need not eliminate every risk of disclosure; patent owners need not guarantee that every embodiment is disclosed; copyright owners need not prove novelty. The law asks instead whether the owner acted reasonably under the circumstances.⁷

Artificial intelligence complicates that inquiry. Modern AI systems are rarely static. They are updated, retrained, integrated into new workflows, connected to third-party platforms, and deployed through autonomous

agents. They depend on extensive datasets, complex architectures, proprietary prompts, model weights, retrieval systems, and human oversight. Assets of real economic value are often distributed across many technical and organizational layers, where traditional asset management never thought to look.³

This article takes up those issues. Its central thesis is that while perfection is not required, reasonable measures in the age of artificial intelligence increasingly require more than confidentiality agreements, access controls, or filing procedures. Organizations must be able to demonstrate governance, documentation, monitoring, evidence preservation, and accountability. As AI systems grow more capable and more consequential, independent assurance may become one of the most persuasive forms of evidence that an organization exercised reasonable measures over its AI assets — a forecast this article develops rather than a rule any court has yet announced.⁵

The Historical Concept of Reasonable Measures

The concept of reasonable measures did not originate with artificial intelligence. It runs throughout intellectual property law and other disciplines concerned with valuable assets. It rests on a simple recognition: absolute protection is rarely possible, so the law asks for conduct that is reasonable under the circumstances. What counts as reasonable evolves as technology, business practice, and risk change.

Trade Secret Protection

Trade secret law offers the clearest illustration. Unlike patents, registered trademarks, or copyrights, trade secret protection does not arise through government filing. It depends on

the owner's efforts to maintain secrecy. Under the Uniform Trade Secrets Act, information qualifies as a trade secret only if it derives economic value from not being generally known and is subject to efforts that are reasonable under the circumstances to maintain secrecy. Those efforts have traditionally included confidentiality agreements, restricted access, physical security, employee training, and contractual protection.⁷

The law does not demand perfection. Businesses operate in practical environments where some risk is unavoidable, and the question is whether the organization behaved reasonably, given the nature and value of the information. That standard — reasonableness, not perfection — carries directly into the AI setting, and it is the thread that ties this article together.

Patent Protection

Patent practice reflects a closely related discipline. Patent rights depend on careful management of invention disclosures, development activity, and filing strategy. Organizations establish invention review committees, disclosure procedures, documentation requirements, and portfolio management systems that preserve patentability and reduce the risk of inadvertent disclosure. Artificial intelligence reshapes that environment, because AI now assists in software development, technical design, research, simulation, and ideation — forcing organizations to consider how invention records and AI-generated contributions interact with traditional patent objectives.

Copyright Protection

Copyright law has focused on authorship, ownership, and creative expression. As such, organizations routinely keep records of the creation of software, documentation, marketing materials, and training content. Generative AI adds difficulty. Organizations increasingly seek to document human involvement in creation,

preserve version histories, and distinguish human-created from AI-generated contributions — practical business steps that serve regardless of how the law ultimately develops.

Information Governance and Cybersecurity

Outside intellectual property law, reasonable measures are deeply embedded in cybersecurity and information governance. Organizations implement frameworks that identify valuable assets, classify risk, control access, monitor activity, document incidents, and maintain audit records. Those frameworks were not built for AI, but they supply useful precedent for AI governance — an analogy that recurs throughout this article.

Why Artificial Intelligence Changes the Analysis

Artificial intelligence does not discard the traditional concept of reasonable measures. It enlarges it. AI systems depend on interconnected assets — training data, architectures, algorithms, code, prompts, retrieval systems, evaluation frameworks, governance processes, and deployment infrastructure — many of which hold economic value independent of the final application, and some of which remain invisible within conventional asset management.^{1,2,3}

Physical AI broadens the discussion again. Autonomous systems generate continuous records of sensor inputs, system states, machine decisions, software versions, and operator interactions. After an accident, failure, insurance claim, regulatory inquiry, or lawsuit, those records can become critical evidence. Preserving them may prove as important to AI governance as invention records have long been to patent practice.

AI Assets Require Reasonable Measures

Artificial Intelligence as Enterprise Capital

The earlier articles advanced a proposition worth restating: artificial intelligence should be viewed as a form of intellectual property and enterprise capital. AI systems satisfy the characteristics traditionally associated with valuable intangible assets as they can be identified, controlled, measured, licensed, transferred, and monetized. And in many organizations, they contribute directly to revenue, efficiency, competitive differentiation, and enterprise value.^{1,2}

Recognizing AI as an asset creates a governance obligation, as valuable assets require management. Just as organizations inventory physical property, maintain patent portfolios, protect trade secrets, and monitor financial holdings, they must establish mechanisms for governing AI. Without governance, they may likely face avoidable risks in ownership, protection, valuation, compliance, and accountability.

Understanding the AI Capital Stack™

Organizations often speak of artificial intelligence as if it were a single asset. In practice, a modern AI system is a set of interdependent layers, each with distinct legal, economic, and operational characteristics — what the AI as IP™ framework calls the AI Capital Stack™. Five categories usually form the foundation: training data, model assets, algorithmic frameworks, computational infrastructure, and deployed applications. Above these sit secondary assets such as prompt libraries, retrieval-augmented generation architectures, evaluation systems, synthetic data generators, autonomous agent frameworks, and governance models.³

Ownership, Control, and Asset Visibility

Traditional intellectual property governance often addressed a narrow set of assets: patent portfolios, copyright registrations, trade secret programs, and licenses. Artificial intelligence widens that universe considerably. Consider a modest generative AI deployment where the organization may hold proprietary training data, licensed third-party data, model customizations, prompt libraries, workflow templates, evaluation frameworks, deployment infrastructure, governance procedures, and customer-facing applications. Each component may carry independent value, require different protection, and sit under a different contract.

The Governance Imperative

Identifying AI assets is not merely an inventory exercise. It is the foundation on which every later measure depends. An organization cannot protect assets it cannot identify, establish ownership of assets it has never documented, preserve value in assets it does not monitor, or credibly claim responsible governance over assets that remain invisible to management. The first reasonable measure in any AI governance framework is therefore visibility: knowing what AI assets exist, how they are used, who controls them, and why they matter.

The AI Asset Inventory as the Foundation of Reasonable Measures

The Importance of Asset Identification

Few organizations would operate without a record of their major physical assets, significant customers, financial accounts, or patent holdings. Yet many deploy artificial intelligence with no comparable inventory. The first step in

exercising reasonable measures over any asset is knowing that the asset exists. Identification is not one component of governance among many; it is the prerequisite for everything that follows.

The AI Asset Register

The practical mechanism for visibility is the AI Asset Register, which functions much like a patent portfolio database, a fixed-asset ledger, or an information governance inventory. It provides a structured record of the AI assets an organization owns, controls, licenses, or uses. Implementation varies, but an effective register generally documents asset name, category, ownership status, responsible business unit, development history, deployment status, licensing restrictions, applicable protections, valuation, and governance controls.

Asset Classification

AI assets do not carry equal importance, so reasonable measures should be calibrated to value and risk. A workable scheme classifies assets as strategic, proprietary, confidential, or public. Classification lets an organization apply controls proportionate to risk — not every asset warrants the same oversight — while remaining able to explain why each governance decision was made.

Asset Lineage and Documentation

Modern AI assets have complex origins. Training data may come from many sources; a model may begin as an open-source foundation and then be fine-tuned on proprietary information; prompt libraries and workflow architectures may evolve through many contributors over long periods. Documenting lineage, therefore, matters. Organizations should keep records of data provenance, licensing rights, contributors, model versions, validation activity, deployment dates, and material modifications.

Why Inventory Is a Reasonable Measure

The value of an AI inventory extends beyond efficiency. Identification itself becomes evidence. When regulators, investors, insurers, counterparties, or courts examine an organization's AI governance, one of the first questions is the most basic: what AI assets did the organization possess, and how did it manage them? An organization that can answer clearly has already demonstrated a measure of reasonableness.

AI Governance as Evidence of Reasonable Measures

Governance Does Not Create Intellectual Property Rights

Intellectual property rights arise from law, not governance. A patent is created through the patent system; copyright arises from qualifying authorship embodied in a tangible medium; trade secret protection originates in legally protectable confidential information. Governance creates none of these, but does serve as evidence that an organization treated its intellectual property as valuable and worthy of protection. It helps preserve, defend, and enforce rights that the law confers.

Governance as a Source of Evidence

Effective governance generates records: approvals, usage logs, version histories, validation reports, audit findings, access records, oversight documentation, training records, incident reports, and policy acknowledgments. Those materials become important when an organization later faces a dispute, investigation, transaction, or insurance claim. Governance therefore performs a dual function — it helps

manage assets today while creating a record that may be relied on tomorrow.

Governance as Enterprise Asset Stewardship

Where AI constitutes material enterprise capital, its governance is not merely a technical concern but a component of enterprise stewardship requiring executive and board attention. The trajectory mirrors cybersecurity, which organizations once delegated to technology staff and which, over two decades, became a governance issue demanding board oversight, executive accountability, insurance review, and regulatory attention. Artificial intelligence is following the same path.^{2,4}

Governance Across Three Levels

Effective AI governance operates on at least three levels. Operational governance manages day-to-day activity. Management governance translates objectives into oversight structures. Board governance provides accountability. As AI becomes increasingly material to enterprise value, expectations at the board level will continue to expand.^{2,4}

Governance and the Future of Reasonable Measures

The traditional conception of reasonable measures centered on protecting information. Modern AI governance asks for more: that an organization understand the assets it controls, exercise oversight over them, document its activities, and monitor the evolving risks of deployment.

AI Disclosure Controls

The Emergence of AI Disclosure Risk

Traditional governance developed around identifiable disclosure events. Organizations

generally knew when information was shared with a counterparty, disclosed in a transaction, provided to a consultant, published, or sent through a formal channel. Artificial intelligence changes that. Employees interact with AI systems constantly, entering prompts, uploading documents, sharing datasets, requesting analyses, generating code, and creating content, often thousands of times a day across an enterprise, and frequently without recognizing that a disclosure has occurred.

AI Platform Classification

Not all AI environments carry the same risk. A sound program distinguishes consumer, enterprise, and private systems. Consumer-facing platforms usually present the greatest challenge, because users have limited visibility into retention, training policies, access controls, data segregation, audit mechanisms, and ownership. Enterprise and private systems typically offer stronger contractual and technical protection.

Approved-Use Policies

Many organizations now adopt formal AI-use policies addressing approved platforms, approved use cases, prohibited disclosures, security requirements, intellectual property concerns, documentation expectations, and escalation procedures. The purpose is not to prevent AI use, but to align that use with company governance objectives.

Escalation and Approval Controls

Some information warrants heightened review before it reaches an AI system: unfiled inventions, proprietary algorithms, trade secret information, acquisition strategy, litigation materials, sensitive customer data, or confidential technical specifications. Escalation controls route these categories through appropriate review rather than leaving the judgment to a single employee at a keyboard.

Documentation as a Reasonable Measure

Disclosure controls derive much of their value from documentation. Records of which platforms were approved, who authorized their use, what training was conducted, when reviews were conducted, and how decisions were made turn governance from an abstract policy into demonstrable conduct. The difference between claiming reasonable measures and showing them is critical.

Patent, Copyright, and Trade Secret Applications

The preceding sections treated artificial intelligence as a collection of valuable assets subject to governance, documentation, and oversight. A more practical question follows: how do reasonable measures apply to the traditional forms of intellectual property that organizations most want to protect?

Patent Governance and AI-Assisted Innovation

Patent systems are built on documentation. Inventors identify ideas, organizations evaluate them, applications are filed, and ownership is established through a formal legal process. Artificial intelligence increasingly participates in the work that precedes filing. AI is used for literature review, evaluation of technical options, code generation, design simulation, concept testing, and the development of alternative embodiments. Organizations should keep records of invention disclosures, dates of conception and development, AI-assisted research, technical contributors, model usage during development, document retention, and filing decisions, all of which establish the chronology of innovation and preserve evidence about the development process.

Documentation and Patent Reasonable Measures

The laboratory notebook was once the principal instrument for documenting innovation. Its modern equivalent is distributed across development repositories, engineering records, model histories, project documentation, simulation outputs, and collaboration platforms. The evidentiary purpose is unchanged; only the location has moved.

Copyright Governance and Human Creativity

Copyright raises a different set of issues. Generative AI has focused attention on authorship, ownership, and creative contribution as organizations use AI to produce software, marketing materials, technical documentation, training content, and audiovisual works. Documenting the full extent of human creative involvement is becoming a deliberate practice rather than an afterthought.

Software Development and Vibe-Coding Controls

AI-assisted software development deserves particular attention. Coding assistants now generate substantial portions of software, and in some organizations, AI-generated code is a routine part of the workflow. Reasonable measures do not require prohibiting AI-assisted coding; they call for governance that documents development activity and supports responsible review, so that the organization understands the provenance and protectability of the code it ships.⁸

Trade Secret Governance in an AI Environment

Trade secret protection may be the area most affected by artificial intelligence. Because it depends so heavily on the owner's efforts to maintain secrecy, and because AI creates new pathways for information to move through

and outside an organization, the controls that matter increasingly resemble a modern access-and-classification program: approved AI platforms, disclosure restrictions, access management, data classification, user training, contractual safeguards, and audit procedures. The underlying principle is the one stated at the outset: an organization seeking protection should be able to show that it treated valuable information as valuable information.⁷

Input-Side Risk: Third-Party Rights and Ownership Exposure

The sections above concern the protection of the organization's own assets. A complete view of reasonable measures also looks the other way; at the risk those assets create. AI systems trained on third-party data may raise infringement and licensing exposure, and AI-generated outputs may carry uncertain ownership. A body of code or content produced largely by a model may enjoy weaker protection than its human-authored equivalent, and may in some circumstances implicate the rights of others. Reasonable measures, therefore, include diligence on training-data provenance and licensing, review of output ownership and clearance, and documentation of human contribution sufficient to support the rights the organization intends to claim. Governance that protects assets on the way out should also screen liability on the way in.

Intellectual Property Governance as Evidence

Patent, copyright, and trade secret protection differ in many respects, yet all three increasingly turn on evidence generated through governance. That evidence includes records demonstrating ownership, authorship, inventorship, confidentiality efforts, disclosure controls, oversight, and stewardship.

Physical AI and the Expansion of Reasonable Measures

Artificial intelligence is entering a new stage. Much of the public conversation has centered on information-based applications — content generation, software development, search, analytics, decision support — that operate within digital environments, where failure tends to be economic, contractual, reputational, or intellectual-property related.

A different category of risk appears when AI leaves the screen. Physical AI controls machines that move, lift, drive, navigate, inspect, manufacture, monitor, and interact with people and property: autonomous vehicles, warehouse robotics, industrial automation, healthcare technologies, drones, construction equipment, and intelligent infrastructure. This physical interaction presents an additional set of governance challenges.

From Information Risk to Physical Risk

The distinction matters. Historically, AI disputes involved copyright, training-data disagreements, licensing, disclosure, trade secret claims, and business losses. Physical AI adds bodily injury, property damage, operational interruption, environmental impact, regulatory scrutiny, insurance claims, and litigation. The stakes change in kind, not merely in degree.

Physical AI Expands the Meaning of Reasonable Measures

In earlier technology, reasonableness was measured by whether information was protected, disclosures were controlled, and records were kept. Physical AI adds new questions. Was deployment appropriately managed? Were operational limits documented? Was human oversight established? Were updates controlled? Were critical records preserved?

Functional Safety Governance

Safety-related governance grows in importance. Organizations deploying Physical AI may need to document testing procedures, validation activity, operational design domains, deployment limitations, performance assumptions, and safety controls.

Human Oversight as a Governance Function

Autonomy does not eliminate the need for human judgment. Organizations must determine when human intervention is required, who holds override authority, what escalation procedures exist, what training is required, and how exceptions are handled.

Model Change Control and Operational Accountability

Unlike conventional machinery, AI-enabled systems change over time through software updates, model revisions, retraining, and parameter adjustments. Governance therefore requires disciplined change management. There must be records of model versions, software updates, deployment dates, validation results, retraining activity, and operational modifications.

Incident Readiness and Evidence Preservation

The most consequential Physical AI governance issue is evidence. These systems generate extensive telemetry, including sensor inputs, perception outputs, decision pathways, software versions, actuator commands, and operator interactions that often exist before anyone anticipates a dispute and may be lost if not preserved promptly.

The Future of Reasonable Measures

Physical AI does not replace traditional intellectual property concerns; it draws them

together. Intellectual property protection, safety management, insurance readiness, incident response, and evidentiary preservation become closely connected activities within a single governance structure.

AI Evidence Preservation

The Expanding Definition of Evidence

Many important AI decisions occur inside complex technical environments that are hard to observe after the fact. Organizations often assume digital systems retain sufficient records automatically. In practice, AI-related information may be overwritten, deleted, modified, replaced, or rendered inaccessible through ordinary operations. What is not deliberately preserved may simply be gone.

Categories of AI Evidence

AI evidence falls into four broad categories. Data evidence includes training datasets and retrieval databases. Model evidence includes model versions and fine-tuning records. Workflow evidence includes prompt libraries and agent instructions. Governance evidence includes policies, audits, risk assessments, and incident reports.

The AI Asset Register as the Modern Laboratory Notebook

For generations, inventors kept notebooks documenting experiments, observations, failures, refinements, and discoveries. The AI Asset Register of Section IV plays a similar role in the AI era. Rather than documenting a single invention, it documents an evolving ecosystem of assets over time.

Preservation of AI-Assisted Innovation Records

As researchers use AI for literature review, software development, technical analysis, simulation, design exploration, and concept generation, preserving the records of that work becomes part of protecting the innovation it produces.

Physical AI and the Rise of Machine Evidence

Evidence preservation perhaps matters most in Physical AI. Autonomous vehicles, robots, industrial systems, infrastructure controls, drones, and intelligent devices generate extensive machine records. The machine records what it observed, what it concluded, and what it did, often before anyone knows an incident has occurred. That characteristic sets Physical AI apart from earlier technology disputes.

Evidence Preservation and Independent Assurance

Preservation also underwrites assurance. Organizations describe their governance through policies, reports, and public disclosures, and the independent assessment of those claims requires evidence. Without preserved records, it is difficult to verify governance activity, model oversight, validation, training practices, disclosure controls, or operational monitoring.⁵

Evidence Preservation as a Reasonable Measure

Most governance controls are designed to prevent problems. Evidence preservation serves a different purpose. Its function is to ensure that when questions arise — and for consequential systems, they eventually do — the organization can answer them.

Application to Intellectual Property Governance

Each principle maps onto reasonable measures. Independence speaks to objectivity. Measurability speaks to evidence. Auditability speaks to review. Comparability speaks to market discipline. Continuous updating speaks to the pace of AI change. Accountability speaks to responsibility for the evaluation itself.⁵

AI Governance Ratings and Assurance Infrastructure

From Governance to Measurement

Markets routinely develop ways to evaluate important but hard-to-observe activity. Credit ratings assess creditworthiness; cybersecurity ratings assess relative security maturity; environmental, social, and governance metrics describe corporate practice. AI governance may be undergoing a similar evolution — though, as with those precedents, methodology and comparability will take time to mature, and early ratings should be read with that caution.

Governance Ratings as Enterprise Infrastructure

A governance rating attempts a standardized assessment of AI governance maturity, examining such factors as asset identification, governance frameworks, oversight structures, disclosure controls, validation processes, monitoring systems, and evidence-preservation practices. Such assessments can support board oversight, investor diligence, insurance underwriting, strategic transactions, and enterprise risk management.⁴

Governance Ratings and Reasonable Measures

A rating does not create intellectual property rights, nor does it guarantee that losses or disputes will not occur. What it can provide is evidence that an organization engaged in a structured, measurable governance process. To the extent a future dispute asks whether reasonable measures were implemented, an independent assessment may become relevant evidence — again, a reasoned expectation rather than an established rule.

Litigation, Transactions, and Evidentiary Applications

Litigation

Disputes turn on conduct. Courts, regulators, insurers, and counterparties seek to determine what was known, who was responsible, what controls existed, and whether those controls were reasonable. Governance records discussed speak directly to those questions. Trade secret disputes examine confidentiality controls; patent disputes examine invention documentation; copyright disputes examine records of creative development; and Physical AI disputes require telemetry, operational records, and evidence of deployment controls.

Transactions and Due Diligence

Artificial intelligence increasingly shapes mergers, acquisitions, investments, and partnerships, as buyers and investors seek evidence of ownership, control, governance maturity, regulatory exposure, and operational risk. An organization with strong governance can more readily demonstrate the existence and quality of its AI assets and negotiate from a position of documented strength.

Insurance and Risk Transfer

Insurers increasingly treat governance as part of risk assessment, examining validation programs, oversight structures, retention practices, incident-response capability, and controls before a loss occurs. Governance can influence not only legal outcomes but also the availability and pricing of risk transfer itself.

A Reasonable Measures Maturity Model

Organizations vary widely in their AI governance capability. The model below offers one way to gauge progress — not a certification, but a self-assessment ladder an organization can use to locate itself and set direction.

LEVEL	LABEL	COMMON CHARACTERISTICS
1	Ad Hoc AI	Limited visibility, minimal governance, informal practices, inconsistent documentation.
2	Policy-Based AI	Written policies, disclosure guidance, basic oversight procedures.
3	Governed AI	AI inventories, ownership records, documentation standards, approval procedures, and monitoring processes.
4	Assured AI	Audits, testing, evidence preservation, independent review, and executive accountability.
5	Physical AI Ready	Telemetry preservation, functional-safety governance, change-control systems, incident-response readiness, independent assurance, board-level oversight.

Conclusion

The history of intellectual property law is, in large part, the history of adapting settled principles to new technology. Patents adapted to industrial innovation. Copyright evolved to meet new forms of creative expression. Trade secret law has adapted to more sophisticated methods of managing information. Artificial intelligence is the next chapter in that progression.^{1,2,3}

The central proposition of the AI as IP™ framework is that artificial intelligence increasingly functions as intellectual property and enterprise capital. If that is right, organizations must consider how those assets are identified, protected, managed, monitored, and preserved. This article has argued that the answer lies in reasonable measures. Once centered on controlling information, reasonable measures now encompass governance, documentation, oversight, monitoring, evidence preservation, and accountability.

Physical AI broadens the concept further because AI now influences people, property, infrastructure, and operations. Governance becomes a mechanism not only for protecting intellectual property but for establishing accountability when intelligent systems act in the physical world.

Independent assurance may represent the next stage. Frameworks such as the Chicago Principles suggest that governance will increasingly be judged not by the existence of policies but by measurable evidence that those policies operate in practice.

Artificial intelligence is increasingly treated as intellectual property. Intellectual property requires reasonable measures. Reasonable measures increasingly require governance. Governance increasingly requires independent assurance. And independent assurance may become the most persuasive evidence that an organization identified, protected, managed, monitored, and preserved its AI assets with the rigor a mature enterprise is expected to bring.

Acknowledgments

J.S. Held thanks James E. Malackowski and Joel Lutzker for providing insight and expertise that greatly assisted this research.

[James E. Malackowski](#) is the Chief Intellectual Property Officer (CIPO) and IP Practice Leader at J.S. Held and Co-founder and Senior Managing Director of Ocean Tomo, a part of J.S. Held. He has served as an expert on more than 100 occasions involving intellectual property economics, including valuation, royalties, lost profits, price erosion, licensing terms, venture financing, copyright fair use, and injunction equities. His work spans AI as IP™, intellectual property valuation, AI governance, AI disputes, and the economics of intangible assets. He is a co-founder and member of the Board of Directors of AIQA Global.

[Joel E. Lutzker](#), Esq., is a Managing Director in the IP Advisory department of Ocean Tomo, a part of J.S. Held, with more than 50 years of experience in patent litigation and transactions. His experience includes the intellectual property aspects of major M&A transactions, licensing and patent acquisitions, financial services intellectual property issues, and international matters involving US/Europe and US/Asia disputes and transactions. He is admitted in New York and Connecticut, before the United States Patent and Trademark Office, and in numerous federal courts. He is a co-founder and member of the Board of Directors of AIQA Global.

Footnotes

1. James E. Malackowski and Eric T. Carnick, "[AI as Intellectual Property: A Strategic Framework for the Legal Profession](#)," J.S. Held Perspectives, 2025.

2. James E. Malackowski and Eric T. Carnick, "[AI as IP™: A Framework for Boards, Executives, and Investors](#)," J.S. Held Perspectives, 2025.

3. James E. Malackowski, David Ngo, and Eric T. Carnick, "[AI as IP™ Framework: A Practical Guide for SMEs to Classify, Protect, and Monetize AI Assets](#)," J.S. Held Perspectives, 2026.

4. James E. Malackowski, J. Scott Womack, and John A. Hudson, "[AI Washing and the Imperative for Board Governance](#)," J.S. Held Perspectives, 2026.

5. AIQA Global, "[The Chicago Principles for Independent AI Assurance](#)" (and accompanying release, "[AIQA Global Publishes the Chicago Principles for Independent AI Assurance](#)"), 2026.

6. [Uniform Trade Secrets Act § 1\(4\)](#).

7. Jacob Golan, Christopher Cowles, and George Chaclas, "[Submitting Ideas to AI Platforms May Affect Patent Rights](#)," Law360, May 20, 2026.

8. Ivan Moreno, "['Vibe Coding' Pushes Cos. to Rethink Copyright Protection](#)," Law360, July 29, 2026.

Publication note

This article is prepared for educational and general information purposes only. It is not intended as legal, accounting, investment, insurance, or regulatory compliance advice. J.S. Held is not a law firm and does not provide legal advice. J.S. Held, its affiliates, and subsidiaries are not certified public accounting firms and do not provide audit, attest, or other public accounting services. The views expressed are those of the authors.

Disclosure of interest: the authors are co-founders and members of the Board of Directors of AIQA Global, which publishes the Chicago Principles for Independent AI Assurance referenced in this article.



This publication is for educational and general information purposes only. It may contain errors and is provided as is. It is not intended as specific advice, legal, or otherwise. Opinions and views are not necessarily those of J.S. Held or its affiliates and it should not be presumed that J.S. Held subscribes to any particular method, interpretation, or analysis merely because it appears in this publication. We disclaim any representation and/or warranty regarding the accuracy, timeliness, quality, or applicability of any of the contents. You should not act, or fail to act, in reliance on this publication and we disclaim all liability in respect to such actions or failure to act. We assume no responsibility for information contained in this publication and disclaim all liability and damages in respect to such information. This publication is not a substitute for competent legal advice. The content herein may be updated or otherwise modified without notice.

J.S. Held, its affiliates and subsidiaries are not certified public accounting firm(s) and do not provide audit, attest, or any other public accounting services. J.S. Held is not a law firm and does not provide legal advice. Securities offered through PM Securities, LLC, d/b/a Phoenix IB or Ocean Tomo Investments, a part of J.S. Held, member FINRA/SIPC. All rights reserved.