Programmatic AI Compliance

A System-Level Framework for Continuous AI Governance

AUTHORS

United Regulation

CARVER agents

Parveen Goribidnur

Founder & CEO, United Regulation

Strategic Advisor, DPDPA Forum

B.Tech Computer Systems, University of British Columbia; Public Policy, National Law School of India University; Algorithms, AI & Civil Liberties Fellow, Friedrich Naumann Foundation for Freedom, Berlin

Dr. Venkata Pingali

Co-Founder, Carver Agents

B.Tech Computer Science, Indian Institute of Technology Bombay; PhD, University of Southern California

ABSTRACT

Artificial intelligence systems are increasingly embedded in critical decision-making across sectors such as finance, healthcare, and public infrastructure. However, the compliance mechanisms governing these systems remain rooted in static, manual, and retrospective models that fail to reflect real-world system behaviour. As AI systems evolve continuously through retraining, fine-tuning, and contextual deployment, compliance must also evolve into a dynamic and embedded function. This paper introduces Programmatic AI Compliance, a system-level architecture that integrates compliance directly into the lifecycle of AI systems. Through three core layers - Specification Generation, Compliance Compilation, and Continuous Validation and the fourth, Omnipresent HumanStewardship Layer across the regulatory landscape - we enable real-time alignment between regulatory intent and system behaviour. This approach reduces latency, improves consistency, and enables scalable governance without proportionate increases in human oversight.

1. Introduction

AI systems have transitioned from isolated tools to foundational infrastructure powering enterprise and public decision-making. Unlike traditional software, these systems continuously evolve continuously based on new data, feedback loops, and model updates, making their behavior inherently dynamic. Additionally, the anticipated scale and complexity are expected to be one to three orders of magnitude greater than those of existing systems. At the same time, regulatory frameworks are expanding in response to concerns around bias, accountability, and safety, yet their enforcement mechanisms remain static, episodic, and limited in scope. This creates a structural disconnect between system behavior and compliance processes, leading to increasing operational and regulatory risk. Organizations are forced to rely on manual audits and fragmented interpretations, which cannot scale with system complexity. The need is no longer for better compliance processes, but for a fundamentally different compliance architecture. Programmatic AI Compliance addresses this gap by embedding governance directly into system design and operation.

2. Foundational Frameworks and Context

Programmatic AI Compliance builds at the intersection of established thinking across regulation, policy, technology, and AI ethics. The framework extends and operationalizes principles from four influential paradigms:

2.1 Regulatory Frameworks: Global Data and AI Governance Regimes

AI governance today is shaped by a rapidly evolving set of regulatory frameworks across jurisdictions, including the General Data Protection Regulation, EU Artificial Intelligence Act, and India's Digital Personal Data Protection Act, 2023. Additional regulatory approaches from the United States, Singapore, and Australia contribute to a fragmented but converging global landscape. These frameworks introduce enforceable obligations around data protection, accountability, transparency, and risk classification. However, they are articulated in legal language and require significant interpretation before implementation. Organizations must reconcile overlapping and sometimes conflicting requirements across jurisdictions, increasing operational complexity. Programmatic AI Compliance provides a unifying layer that translates these diverse obligations into structured, executable specifications, enabling consistent enforcement across systems and geographies.

2.2 Policy Framework: NIST AI Risk Management Framework

The NIST AI RMF provides a structured approach to identifying, assessing, and managing AI-related risks across the system lifecycle. It emphasizes governance, mapping, measurement, and management as continuous functions rather than one-time activities. However, its implementation remains largely guidance-driven and dependent on organizational interpretation. Programmatic AI Compliance builds

on this by translating risk management principles into machine-executable specifications and controls, enabling continuous enforcement rather than periodic assessment. This bridges the gap between policy intent and operational execution. It effectively transforms risk management from a governance exercise into a system capability.

2.3 Technology Framework: Policy as Code

Policy as Code has emerged from cloud and DevOps ecosystems as a method of embedding governance rules directly into software systems. It enables automated enforcement of policies such as security, access control, and infrastructure compliance. This approach demonstrates that governance can scale when encoded into executable logic. Programmatic AI Compliance extends this concept into the regulatory domain, where policies are not just technical constraints but legal and ethical requirements. By compiling regulatory specifications into enforceable system logic, it generalizes Policy as Code from infrastructure governance to AI system governance. This creates a foundation for scalable, repeatable compliance across complex environments.

2.4 AI Ethics Frameworks: Global Principles for Trustworthy AI

Global AI governance has been shaped by a convergence of ethical frameworks developed by multilateral organizations, governments, and standards bodies, including the OECD AI Principles, UNESCO Recommendation on the Ethics of Artificial Intelligence, the European Union Ethics Guidelines for Trustworthy AI, and contributions from bodies such as the World Economic Forum. These frameworks converge on core principles such as fairness, accountability, transparency, safety, privacy, and human oversight. While they provide strong normative direction, they lack mechanisms for consistent and scalable implementation.

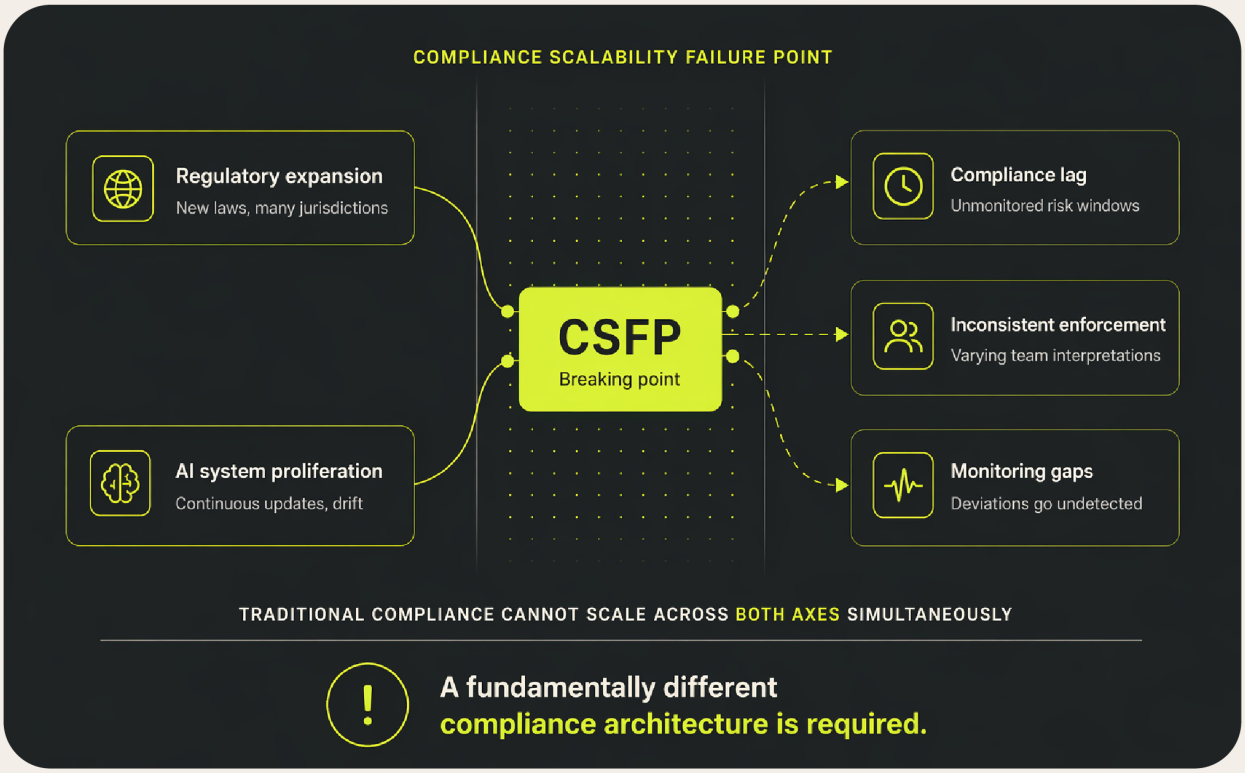
Programmatic AI Compliance operationalizes these principles by embedding them into structured specifications and validation mechanisms, enabling continuous enforcement and measurement. This programmatic approach further enables consistent and potentially interoperable implementation of extensions that are specific to particular geographies or industry sectors.

2.5. Synthesis

While each of these frameworks addresses a critical dimension of AI governance, none independently solves the challenge of continuous, scalable compliance. Programmatic AI Compliance integrates regulatory obligations, policy risk structures, technological automation, and ethical principles into a unified system. This enables regulatory, technical, and ethical requirements to be encoded, executed, and validated in real time. The result is a governance model that matches the scale and dynamism of modern AI systems.

3. System Context: The Breaking Point

AI governance today is caught between two accelerating forces: regulators issuing new obligations faster than organisations can absorb them, and AI systems evolving faster than any manual compliance process can track. The diagram below maps this collision - showing how regulatory expansion and AI proliferation converge on a single structural breakdown, the Compliance Scalability Failure Point, and the three failure modes that result.



3.1 Demand-Side Dynamics: Regulatory Expansion

Regulatory environments globally are experiencing rapid expansion in both scope and complexity, driven by the widespread adoption of AI technologies. New laws and guidelines are being introduced frequently, often with overlapping or conflicting requirements across jurisdictions. Sector-specific regulations further complicate compliance, as different industries prioritize different dimensions such as safety, fairness, or explainability. Organizations must continuously interpret and implement these evolving requirements, often without clear operational guidance. This results in fragmented compliance strategies and increased reliance on legal interpretation rather than system-level enforcement. Additionally, enforcement mechanisms are becoming stricter, increasing the cost of non-compliance. The net effect is a regulatory landscape that is both dynamic and difficult to operationalize.

3.2 Supply-Side Dynamics: AI System Proliferation

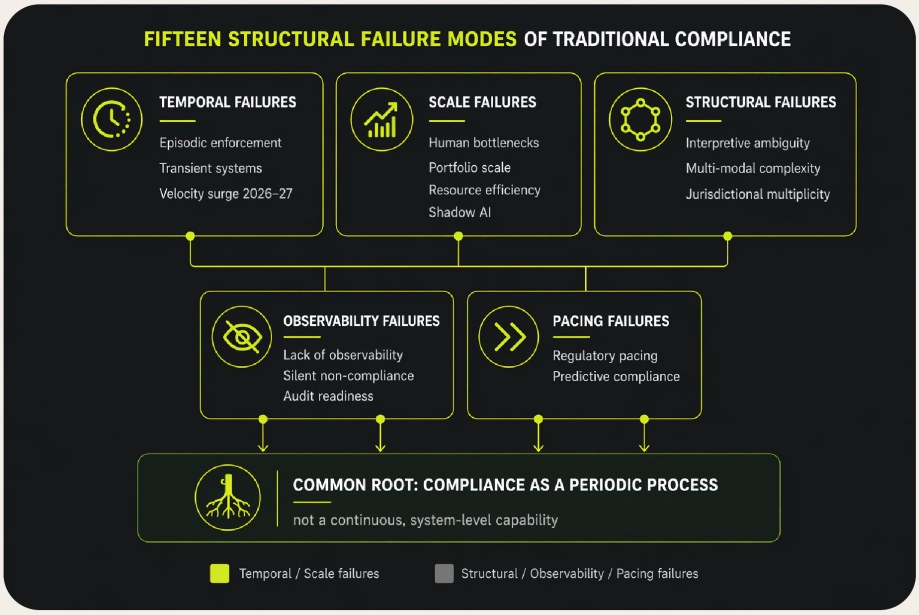
On the supply side, AI systems are being developed and deployed at unprecedented speed and scale. Enterprises now manage large portfolios of AI applications, each with unique models, data sources, and risk profiles. Continuous retraining and updates introduce behavioural drift, where systems deviate from their originally validated state. Deployment across cloud and edge environments further complicates monitoring and control. Development cycles have shortened significantly, leaving limited time for traditional compliance checks. As systems become more autonomous, their decision-making pathways become less transparent and harder to audit manually. This proliferation creates a scenario where compliance must operate across both scale and dynamism simultaneously.

3.3 Compliance Scalability Failure Point (CSFP)

The interaction between regulatory expansion and system proliferation results in a critical breakdown point for traditional compliance models. At this stage, organizations are unable to maintain alignment between regulatory requirements and system behavior across all deployed applications. Compliance processes lag behind system updates, creating windows of unmonitored risk. Interpretations vary across teams, leading to inconsistent enforcement and potential legal exposure. Monitoring mechanisms, where they exist, are often limited in scope and unable to detect subtle deviations. This systemic inability to scale compliance alongside system growth is defined as the Compliance Scalability Failure Point. Addressing this failure requires rethinking compliance as a continuous, system-level capability rather than a periodic process.

4. Limitations of Existing Compliance Systems

Before introducing a better model, it is worth being precise about why the current one breaks. Existing compliance practice fails along six distinct dimensions, spanning both its temporal assumptions - that systems stay stable between audits - and its structural ones - that fragmented, human-dependent processes can scale to match AI deployment. The diagram below maps these six failure modes and the common root they share.



4.1 Episodic Enforcement

Traditional compliance operates through discrete checkpoints such as pre-deployment audits or periodic reviews, assuming system stability between evaluations. However, AI systems evolve continuously, rendering these checkpoints insufficient for capturing real-time behavior. Changes introduced through retraining or environmental shifts can lead to deviations that remain undetected until the next audit cycle. This creates a gap between system operation and compliance validation, increasing risk exposure. Episodic enforcement also lacks responsiveness, as corrective actions are often delayed. As a result, compliance becomes reactive rather than proactive, addressing issues only after they manifest. This model is fundamentally incompatible with continuously evolving systems.

4.2 Human-Centric Bottlenecks

Compliance processes rely heavily on human expertise for interpretation, validation, and enforcement, which limits scalability. As the number of systems increases, the workload on compliance teams grows linearly, creating bottlenecks. Manual reviews are time-consuming and prone to inconsistency, especially when dealing with complex AI behaviours. Additionally, expertise in both regulatory and technical domains is scarce, further constraining capacity. This reliance on human intervention slows down system deployment and adaptation. While human oversight is essential, it cannot serve as the primary mechanism for large-scale compliance. Automation is required to handle repetitive and high-volume tasks.

4.3 Interpretive Ambiguity

Regulatory language is often intentionally broad to accommodate diverse use cases, but this introduces ambiguity in implementation. Different teams may interpret the same requirement differently, leading to inconsistent compliance across systems. Without a standardized method of

translating regulation into system-level constraints, organizations struggle to achieve uniform enforcement. This ambiguity also complicates audits, as there is no single source of truth for compliance interpretation. Over time, these inconsistencies can lead to regulatory disputes or enforcement actions. Resolving ambiguity requires structured translation mechanisms and shared representations of regulatory intent.

4.4 Lack of Observability

Most organizations lack infrastructure to continuously monitor AI system behavior in relation to compliance requirements. Existing monitoring tools focus on performance metrics rather than regulatory alignment. Without real-time observability, deviations from intended behavior may go unnoticed until they cause significant impact. This is particularly problematic for high-risk applications where even small deviations can have serious consequences. Observability gaps also hinder root cause analysis and corrective action. A robust compliance system must include continuous monitoring capabilities that provide visibility into both system behavior and compliance status.

4.5 Fragmented Regulatory Landscape

AI governance is shaped by multiple regulatory frameworks across jurisdictions, each with distinct definitions, risk classifications, and compliance requirements. Organizations operating globally must navigate overlapping and sometimes conflicting obligations, creating complexity in implementation. This fragmentation leads to inconsistent compliance strategies across regions and systems. It also increases the burden of interpretation, as teams must reconcile differences in legal language and enforcement expectations. The absence of standardized representations makes it difficult to operationalize compliance uniformly.

There is a need for a unifying abstraction layer that can translate diverse regulatory requirements into structured, machine-readable specifications. Such a layer should enable consistent interpretation of regulatory intent across jurisdictions while preserving local nuances. It must support the simultaneous encoding of multiple frameworks within a single system architecture to avoid fragmentation. Standardized representations are required to reduce duplication of effort and minimize conflicting implementations. Without this, organizations will continue to face inefficiencies and increased risk in managing cross-jurisdictional compliance.

4.6 Regulatory Pacing Problem

Regulatory frameworks often evolve at a slower pace than technological innovation, particularly in the rapidly advancing field of AI. New capabilities such as generative models, autonomous systems, and adaptive learning mechanisms outpace the development of corresponding regulatory guidance. This creates gaps where emerging risks are not yet fully addressed by formal regulation. Organizations are forced to operate in uncertain environments, relying on internal judgment and best-effort interpretations. The lag also results in reactive policymaking, where regulations are introduced only

after risks have materialized. Bridging this gap requires more adaptive and forward-looking compliance mechanisms that can evolve alongside technology. These compliance mechanisms when made programmable can match technological advancement better.

4.7 Multi-modal Complexity

Existing compliance frameworks were designed for systems with discrete, well-defined inputs and outputs. Modern AI deployments routinely combine vision, language, structured data, and real-time event streams within a single decision pipeline. Each modality introduces its own regulatory surface - a system that ingests identity documents, interprets natural language, and scores behavioural signals simultaneously carries overlapping obligations across data protection, explainability, and fairness regimes. No single audit vector can capture these cross-modal dependencies. Compliance frameworks that evaluate components in isolation will systematically miss the interactions between them, which is precisely where the highest-risk behaviour emerges.

4.8 Compliance at Portfolio Scale

Organisations will no longer manage a handful of AI systems - they will operate portfolios of hundreds to thousands of models across business units, geographies, and deployment environments. Traditional compliance practice treats each system as an independent audit subject, making effort proportional to the number of systems under governance. This does not scale. A team that can adequately audit twenty systems cannot audit two thousand using the same methods, even with proportional headcount increases. The problem is structural: compliance logic is rebuilt from scratch for each system, institutional knowledge does not accumulate, and coverage gaps are inevitable. What is required is a platform model in which compliance logic is authored once, compiled into reusable policy packages, and applied uniformly across the entire portfolio - reducing marginal compliance cost per system as the estate grows rather than increasing it.

4.9 Transient Systems

AI is increasingly deployed in ephemeral configurations - session-scoped agents, serverless inference endpoints, containerised pipelines - that may never persist long enough to complete a traditional audit cycle. A compliance model that assumes a stable, addressable system as its subject breaks down entirely when the system exists for seconds or minutes. Compliance cannot be applied retroactively to something that no longer exists. For transient systems, governance must be embedded at instantiation - specifications compiled into the deployment artifact itself, so that compliance is a property of how the system starts rather than a check applied after it runs.

4.10 Predictive Compliance

Product development cycles have compressed from quarters to weeks. By the time a traditional compliance review flags a regulatory conflict, the architectural decisions that created it are already

locked in - unwinding them is costly and sometimes impossible. Compliance must move earlier in the development pipeline, providing signal at the design stage rather than the deployment gate. This requires specifications precise enough to evaluate system designs against regulatory requirements before code is written, shifting compliance from a post-hoc gate into a design-time input.

4.11 Resource Efficiency

Compliance functions are being asked to govern a larger, faster-moving AI estate with teams that have not grown proportionally. The constraint is not effort - it is structural. Manual compliance processes do not become more efficient with practice; they remain labour-intensive by design. Automation is required not as a convenience but as a necessity. The goal is not to eliminate human judgment but to reserve it for decisions that genuinely require it - ambiguous regulatory interpretation, edge case adjudication, and remediation strategy - while automating the high-volume, repeatable work of monitoring, evidence collection, and policy enforcement.

4.12 Jurisdictional Multiplicity

A single AI system deployed across markets today operates simultaneously under multiple overlapping regulatory regimes - the EU AI Act, GDPR, DPDP, sector-specific rules, and local enforcement guidance - each with distinct definitions, risk classifications, and obligations. The challenge is not merely navigating a fragmented landscape but managing the simultaneous, conflicting demands placed on the same system. A decision that satisfies one jurisdiction's explainability requirement may conflict with another's data minimisation obligation. Without a specification layer capable of encoding and arbitrating these conflicts systematically, organisations are forced into lowest-common-denominator compliance that satisfies no regulator fully.

4.13 Audit as a First-Class Output

Regulators and boards increasingly expect continuous audit readiness - not point-in-time reports assembled retrospectively under examination pressure. Traditional compliance generates evidence as a secondary output of manual processes, which means it is incomplete, inconsistent, and expensive to produce on demand. A programmatic compliance platform inverts this: audit evidence is a byproduct of normal operation, generated continuously as the system monitors, scores, and logs. The audit trail exists before the auditor arrives. This fundamentally changes the organisation's posture from reactive to demonstrably compliant.

4.14 Shadow AI and Third-Party Models

Governance cannot stop at the boundary of internally built systems. Organisations are consuming AI through vendor APIs, embedded foundation models, and third-party pipelines at a scale that outpaces procurement and risk review processes. Shadow AI - models adopted by business units outside formal governance channels - represents a compliance surface that is largely invisible to existing frameworks.

A programmatic approach must extend beyond the systems an organisation builds to encompass the AI it buys, embeds, and inadvertently inherits through its technology stack.

4.15 Regulatory Velocity: The 2026–27 Enforcement Surge

The compliance challenge of previous years was primarily interpretive - understanding what emerging regulations required. The challenge of 2026–27 is operational: the EU AI Act, India's DPDP Act, and a wave of sector-specific AI rules are entering active enforcement simultaneously, compressing the window between regulatory obligation and enforcement action. Organisations that have relied on the ambiguity of transition periods no longer have that buffer. The volume and simultaneity of these obligations arriving at the enforcement stage represents a one-time surge that no manually operated compliance function can absorb. Programmatic compliance is not merely advantageous in this environment - it is the only architecture that can respond at the required speed and breadth.

5. Programmatic AI Compliance Architecture

The preceding sections have established a central finding: the compliance challenge facing organisations today is not one of effort or intent, but of structural capacity. The volume of regulatory obligations, the pace of AI system change, and the scale of deployment portfolios have collectively outrun what any manual or human-centric compliance model can sustain. This is not a temporary resourcing problem. It is a permanent architectural one. Without automation, organisations will be unable to meet their compliance obligations - not because they lack the will, but because the mathematics of coverage, velocity, and scale make it impossible to do so otherwise.

This does not mean that automating compliance is straightforward or risk-free. Encoding regulatory intent into machine-executable specifications introduces its own failure modes: interpretive errors that propagate silently at scale, enforcement logic that satisfies the letter of a requirement while missing its purpose, and an over-reliance on automated systems that can erode the critical human oversight that regulation itself demands. These risks are real and must be managed deliberately. Automation is not a replacement for legal judgment; it is a force multiplier for it - and like any such multiplier, it amplifies errors as readily as it amplifies capacity.

What automation does guarantee, even where it is imperfect, is coverage. A programmatic compliance system that operates with 80% accuracy across a portfolio of one thousand AI applications enforces policy at a breadth and frequency that no team of compliance professionals can replicate manually. As specifications are refined, as feedback loops tighten, and as institutional knowledge accumulates in the platform, that accuracy improves - while coverage continues to grow. The trajectory of programmatic compliance is toward more systems governed, more frequently, against more regulatory requirements, at lower marginal cost per system. The alternative - scaling human compliance effort proportionally with AI deployment - is not a viable path. The architecture described in this section is the path that is.

Programmatic AI Compliance addresses the failures above through a three-layer architecture that embeds governance directly into the AI system lifecycle. Each layer has a specific function: translating

regulatory text into machine-readable specifications, compiling those specifications into enforceable system constraints, and continuously validating system behaviour against those constraints. Human stewardship operates across all three layers, ensuring that automated enforcement remains grounded in legal and contextual judgment.

5.1 Layer 1: High-Trust Specification Generator

This layer converts regulatory text into structured, machine-readable specifications that can be consistently interpreted and applied. Using a combination of AI-assisted parsing and expert validation, regulatory requirements are translated into formal representations that capture conditions, constraints, and permissible variations. These specifications are version-controlled, allowing organizations to track changes in regulatory interpretation over time. By incorporating multiple interpretations where ambiguity exists, the system preserves flexibility while maintaining structure. This layer acts as the foundational source of truth for compliance logic. It ensures that all downstream processes operate on consistent and traceable representations of regulatory intent. Without this layer, compliance remains fragmented and dependent on manual interpretation.

5.2 Layer 2: Compliance Compiler

The Compliance Compiler translates structured specifications into enforceable system-level policies and constraints. It generates guardrails that can be integrated directly into AI systems, ensuring that behavior remains within defined regulatory boundaries. This includes encoding thresholds, decision rules, and monitoring triggers that align with compliance requirements. By decoupling compliance logic from system architecture, the compiler enables reuse of policies across multiple applications. This significantly reduces implementation effort and ensures consistency. The compiler also supports

automated updates, allowing systems to adapt quickly to regulatory changes. This layer transforms compliance from a conceptual requirement into an operational capability.

5.3 Layer 3: Continuous Compliance Validator

The validator continuously monitors system behavior and compares it against defined specifications to ensure ongoing compliance. It captures real-time data on system outputs and evaluates them against constraints and conditions defined in earlier layers. Deviations are detected and flagged immediately, enabling rapid response and mitigation. The validator supports multiple evaluation modes, including passive monitoring and active testing through simulated scenarios. It also generates audit logs that provide traceability and accountability. By operating continuously, this layer closes the gap between system evolution and compliance validation. It ensures that compliance is maintained not just at deployment, but throughout the system lifecycle.

5.4 Omnipresent Human Stewardship

Human oversight remains essential for interpreting complex regulatory requirements and resolving ambiguous cases. Experts validate specifications, ensuring that machine-readable representations accurately reflect legal intent. They also determine applicability of rules to specific systems, particularly in edge cases where automated logic may be insufficient. In the validation layer, humans investigate flagged anomalies and make judgment-based decisions on corrective actions. This hybrid model leverages the strengths of both humans and machines, combining scalability with contextual understanding. By focusing human effort on high-value tasks, organizations can maintain oversight without sacrificing efficiency. The goal is not to replace human judgment, but to augment it with system-level capabilities.

5.5 Roadmap for Programmatic AI Compliance Architecture

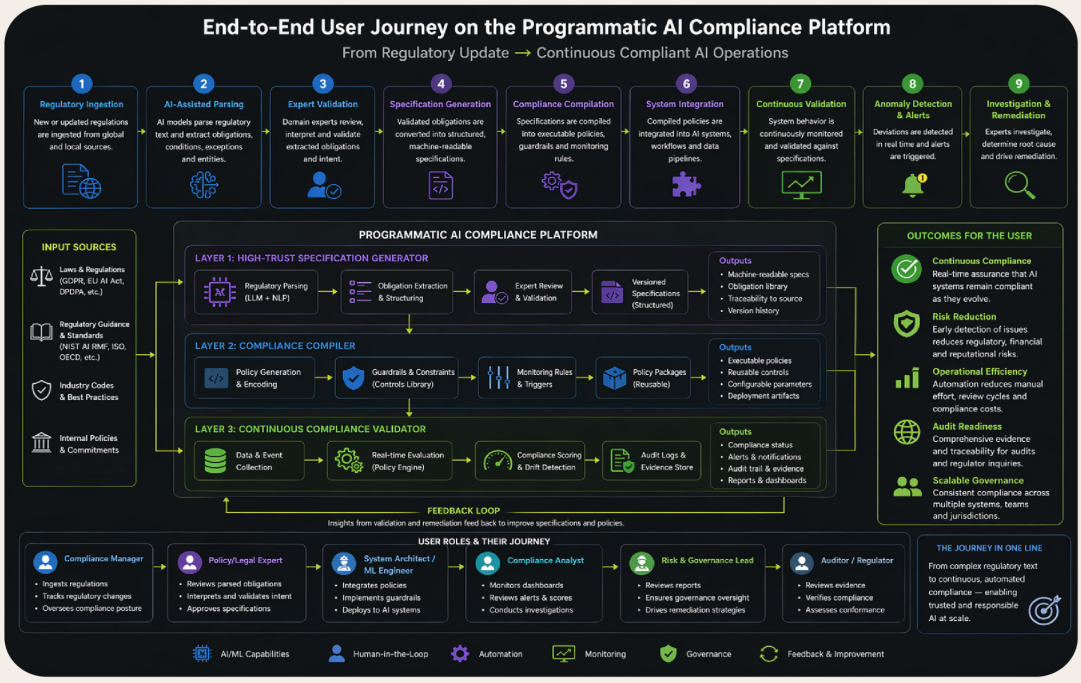
The architecture described in preceding sections establishes the foundational capability for programmatic compliance. Realising its full potential requires extending it across the complete AI development lifecycle - from design-time constraint checking and compliance-embedded test suites through deployment gates that produce signed attestation artifacts, to decommission processes that honour retention and audit obligations as systems are retired. Enforcement mechanisms must be calibrated dynamically rather than configured statically: feedback signals from prior enforcement events, human review outcomes, and evolving regulatory guidance should progressively refine thresholds and scoring weights. Where regulatory language admits multiple plausible interpretations, a structured disambiguation process must encode each alternative alongside its legal rationale and resolution record, defaulting to the most conservative reading until expert determination closes the ambiguity and adds it to the obligation library as accumulated institutional knowledge.

The long-term scalability of programmatic compliance depends on open specification schemas and interoperability standards that allow compliance logic to be exchanged across platforms, vendors, and

regulatory bodies without translation overhead. The PCA roadmap includes publishing internal specification formats as open standards and engaging with industry bodies and regulators to converge on common representations - covering not only the format of obligations but the interfaces between specification generators, compilers, validators, and the AI systems they govern. The compliance platform must itself be subject to a dedicated test framework operating at three levels: specification fidelity against legal intent, compiler correctness across boundary conditions, and validator regression against known violation patterns. A platform that governs AI systems without being rigorously governed itself cannot be trusted at scale.

6. Reimagining the Compliance Function

What the architecture enables, the platform makes operational. Six roles participate across the compliance journey - Compliance Manager, Policy and Legal Expert, System Architect, Compliance Analyst, Risk and Governance Lead, and Auditor - each engaged precisely where human judgment is irreplaceable rather than as a bottleneck in routine enforcement. The feedback loop is what closes the system: anomaly investigation and remediation findings propagate back into the specification layer, tightening interpretations and improving future cycles. Over time, the platform accumulates institutional knowledge - versioned specifications, obligation libraries, reusable policy packages, and audit evidence - that compounds in value across the system portfolio. Compliance ceases to be a function that consumes resources proportional to the number of systems under governance and becomes instead a platform capability with fixed overhead and elastic reach.



The emergence of AI agent systems introduces a structural demand that the compliance function must

meet directly: integration not merely with the outputs of AI development, but with its process. Agent systems are not deployed once and monitored passively - they are composed, orchestrated, and continuously modified by teams operating at engineering velocity. Compliance professionals must therefore be embedded within agent development teams in the same way that security engineers are embedded within product teams under a DevSecOps model. This means compliance specifications are reviewed alongside system design documents, compiled policies are tested as part of the agent's CI pipeline, and the Compliance Analyst role carries the authority to block a release on regulatory grounds with the same standing as an engineering reviewer. The alternative - a compliance function that engages with agent systems only at the point of deployment - will consistently arrive too late, after architectural decisions that create regulatory exposure have already been made and locked in.

7. Risk Evaluation Framework

Any compliance architecture must account for the ways it can fail. Four risks are inherent to programmatic compliance at scale: drift between system behaviour and validated specifications, misalignment between compliance logic and regulatory intent, inability to scale as the system portfolio grows, and silent violations that go undetected without continuous monitoring. Each risk has a corresponding mitigation built into the architecture.

7.1 Compliance Drift

Compliance drift occurs when systems deviate from their validated state due to updates, retraining, or environmental changes. This is a natural consequence of continuous system evolution but poses significant regulatory risk. Without continuous monitoring, drift may go undetected until it results in

adverse outcomes. Programmatic compliance addresses this through real-time validation and drift detection mechanisms. By continuously comparing system behavior against specifications, deviations can be identified early. This allows for proactive mitigation rather than reactive correction. Managing drift is critical for maintaining long-term compliance.

7.2 Interpretive Misalignment

Interpretive misalignment arises when the implementation of compliance logic does not accurately reflect regulatory intent. This can occur due to ambiguity in regulation or errors in translation. Such misalignment can lead to systems that are technically compliant but fail to meet the spirit of the law. Programmatic compliance mitigates this risk by incorporating multiple interpretations and human validation. Structured specifications provide a clear mapping between regulation and implementation. Continuous feedback loops allow for refinement of interpretations over time. This ensures closer alignment between intent and execution.

7.3 Scaling Failure

Scaling failure occurs when compliance processes cannot keep pace with the growth in AI systems. As organizations deploy more systems, manual processes become unsustainable. This leads to gaps in coverage and increased risk exposure. Programmatic compliance addresses this by automating repetitive tasks and enabling reuse of compliance logic. The compiler and validator layers allow organizations to scale compliance without proportional increases in resources. This ensures consistent enforcement across all systems. Scalability is essential for maintaining compliance in large, complex environments.

7.4 Silent Non-Compliance

Silent non-compliance refers to violations that occur without detection due to lack of monitoring or insufficient validation mechanisms. These violations can persist for long periods, increasing risk and potential liability. Programmatic compliance reduces this risk through continuous monitoring and real-time alerting. The validator layer ensures that deviations are detected as soon as they occur. Audit logs provide traceability, enabling investigation and accountability. By making compliance observable, organizations can move from reactive to proactive risk management. Detecting silent failures is critical for building trustworthy AI systems.

8. Implementation Considerations

Implementing programmatic compliance requires integrating new components into existing AI and governance infrastructure, and this integration must reach deeper than surface-level tooling. AI systems designed without compliance interfaces embedded in their architecture will support only shallow enforcement - the compliance platform operating at the boundary of the system rather than within it. Organisations must therefore establish compliance interface standards as a baseline

requirement for all new AI systems and a tracked remediation item for existing ones, alongside the observability pipelines, model metadata registries, and inference logging infrastructure that determine the ceiling of what programmatic enforcement can achieve. Adoption can be incremental, beginning with monitoring capabilities and expanding toward full compilation and lifecycle coverage, but the underlying codebase structures must be aligned from the outset if the platform is to function at depth.

Compliance evidence has no value if it cannot be recovered or trusted under examination. The architecture must maintain immutable, append-only records of compliance events - capturing the specification state, system version, input context, and determination at the time each event occurred - with retention aligned to the longest applicable regulatory obligation across all relevant jurisdictions. This is not an audit convenience; it is increasingly a legal requirement under frameworks that mandate accountability across the full lifecycle of consequential AI decisions. Beyond preservation, evidence must be perennial: generated continuously as a byproduct of normal operation at every lifecycle stage, from design-time specification checks through deployment attestation artifacts to operational monitoring logs, such that the audit trail exists before the auditor arrives and requires no retrospective reconstruction when it is called upon.

9. Ecosystem Implications

Programmatic compliance is not solely an organizational challenge but an ecosystem-level transformation. Regulators must move toward machine-readable frameworks to enable automated interpretation and enforcement. Industry bodies can play a role in standardizing specification formats and best practices. Enterprises must invest in compliance infrastructure as a core capability rather than a support function. Auditors need to transition from periodic reviews to continuous validation models. Collaboration across stakeholders is essential to ensure interoperability and trust. This shift will redefine how compliance is understood and implemented across industries. It represents a move toward a more integrated and scalable governance ecosystem.

10. Limitations

While programmatic compliance offers significant advantages, it is not without limitations. Not all regulatory requirements can be fully formalized, particularly those involving subjective judgment. Historically, semantic heavy domains have seen limited automation for this reason. Automation introduces new risks, including potential errors in specification or enforcement logic. Standardization across jurisdictions remains a challenge, limiting interoperability. There is also a risk of over-reliance on automated systems, which may reduce critical human oversight. Implementation requires significant investment in infrastructure and expertise. These limitations must be acknowledged and addressed through careful design and governance. Continuous refinement will be necessary as the field evolves.

11. Conclusion

AI systems have fundamentally changed the nature of technology, requiring a corresponding transformation in how they are governed. Traditional compliance models, designed for static systems, are no longer sufficient to manage dynamic and scalable AI environments in which hundreds of models may be deployed, updated, and retired in the time it takes to complete a single manual audit cycle. The conclusion is unavoidable: without automation, organisations cannot meet their compliance obligations at the scale and velocity that modern AI deployment demands. The gap between regulatory requirement and enforcement capacity will only widen if compliance remains a labour-intensive, episodic function.

This is not to say that automation resolves the compliance problem cleanly. Encoding regulation into executable logic introduces risks that are distinct from those of manual processes but no less serious: specification errors that propagate uniformly across a large portfolio, enforcement logic that satisfies technical criteria while missing regulatory intent, and the structural risk that automation creates a false sense of assurance that displaces the human oversight it was designed to support. Programmatic compliance must be designed with these failure modes in view. The architecture described in this paper addresses them through layered human stewardship, interpretive validation, and feedback mechanisms that allow the system to improve over time - but they cannot be assumed away. Imperfect automation, deployed without adequate governance of the automation itself, can be worse than the manual processes it replaces.

What automation guarantees, however - even where it remains imperfect - is an expansion of coverage that no manual model can match. A programmatic compliance platform that monitors one thousand applications enforces policy at a breadth and frequency that is categorically beyond the reach of human teams operating at scale. Each refinement to a specification, each tightening of a feedback loop, each accumulation of institutional knowledge in the platform's obligation library improves the quality of enforcement while the coverage continues to grow. Over time, the marginal compliance cost per application falls as the portfolio expands - the inverse of the trajectory that manual compliance follows. Programmatic AI Compliance offers a new paradigm, embedding governance directly into system architecture, and shifting compliance from a process that consumes resources proportionally to the number of systems governed into a platform capability with fixed overhead and elastic reach. The future of AI governance will depend on exactly this ability to operationalize regulation at the same scale and speed as the technological systems it governs.

References

Regulatory Frameworks

- General Data Protection Regulation. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council.
- EU Artificial Intelligence Act. (2024). Regulation laying down harmonised rules on artificial intelligence.
- Digital Personal Data Protection Act, 2023. (2023). Government of India.
  AI Verify Framework. (2022). Government of Singapore.
- Blueprint for an AI Bill of Rights. (2022). The White House Office of Science and Technology Policy.
  Australia AI Ethics Principles. (2019). Australian Government.

Policy & Risk Frameworks

- NIST AI Risk Management Framework. (2023). National Institute of Standards and Technology.
- OECD AI Principles. (2019). Organisation for Economic Co-operation and Development.

AI Ethics & Governance Frameworks

- UNESCO Recommendation on the Ethics of Artificial Intelligence. (2021). UNESCO.
- European Union Ethics Guidelines for Trustworthy AI. (2019). European Commission High-Level Expert Group on AI.
- World Economic Forum. (2023). AI Governance: A Holistic Approach.

Standards & Technical Foundations

- ISO/IEC 42001. (2023). International Organization for Standardization.
- ISO/IEC 23894. (2023). ISO.
- Policy as Code. Concept widely adopted in DevSecOps and cloud governance ecosystems.
- Continuous Compliance. Emerging paradigm in cybersecurity and infrastructure governance.

Foundational Literature

- Lawrence Lessig. (1999). Code and Other Laws of Cyberspace.
- Cathy O'Neil. (2016). Weapons of Math Destruction.
- Virginia Eubanks. (2018). Automating Inequality.

Author Contribution

- Goribidnur, P., & Pingali, V. (2026). The Case for Programmatic AI Compliance: A System-Level Framework for Continuous AI Governance.

A JOINTLY PUBLISHED RESEARCH PAPER

Programmatic AI Compliance

Embedding governance at the speed of AI

A framework for continuous, scalable,and automated regulatory compliance across the AI system lifecycle.

PUBLISHED BY

UnitedRegulations & Carver Agents

VERSION 1.2 | APRIL 2026

End of Document