

# ***The Governability Gap under the EU AI Act: Compliance Without Governability in Autonomous Systems***

Author: Andreas Blumer

## **Abstract**

Autonomous systems increasingly operate across extended runtime lifecycles characterized by continuous adaptation, environmental change and growing operational complexity. While the EU AI Act establishes extensive requirements concerning transparency, accountability, human oversight, risk management and post-market monitoring, relatively little attention has been devoted to situations in which systems remain formally compliant while progressively losing the practical capacity to support these objectives throughout runtime operation.

This paper introduces the concept of the **Governability Gap**, defined as the discrepancy between formal compliance status and the practical governability of an autonomous system. The paper argues that compliance and governability represent distinct concepts. Compliance describes the extent to which regulatory requirements have been satisfied, whereas governability describes the extent to which systems remain observable, traceable, controllable, auditable and accountable throughout operation.

Building upon previous work on Governability by Design and Regulatory Continuity, the paper explores how governability may deteriorate despite the continued satisfaction of formal compliance requirements. Sources of governability degradation including increasing operational complexity, runtime adaptation, distributed coordination, environmental evolution and emergent behavior are examined.

The paper further proposes that the Governability Gap may function as a leading indicator of future compliance degradation. As governability decreases, the ability to sustain transparency, accountability, oversight and risk management may progressively weaken, increasing the likelihood that regulatory objectives become difficult to maintain over time.

The central argument advanced is that future autonomous systems may not fail because compliance requirements are absent, but because the governability required to preserve those requirements gradually erodes during runtime operation. Understanding, identifying and addressing the Governability Gap may therefore become essential for maintaining regulatory continuity within increasingly autonomous technological ecosystems.

## **Keywords**

Governability Gap, Governability, EU AI Act, Regulatory Continuity, Continuous Compliance, Runtime Governability, Autonomous Systems, Governance Infrastructure, Human Oversight, Accountability, Auditability, Observability, Traceability, AI Governance

# 1. Introduction

The emergence of increasingly autonomous systems is transforming how societies, organizations and regulatory institutions approach governance, accountability and technological oversight. Autonomous systems are no longer confined to static operational environments. Instead, they increasingly operate across extended runtime lifecycles, interact with dynamic environments, coordinate with distributed systems and adapt to evolving operational conditions.

These developments have contributed to growing regulatory attention. The European Union Artificial Intelligence Act (EU AI Act), alongside related governance and assurance initiatives, seeks to establish mechanisms that promote transparency, accountability, human oversight, risk management and trustworthiness throughout the lifecycle of AI-enabled systems.

Underlying many of these efforts is a fundamental assumption.

If a system satisfies regulatory requirements, it is often implicitly assumed that the system remains sufficiently governable throughout operation.

In practice, compliance and governability are frequently treated as closely related or even interchangeable concepts. Systems that successfully complete conformity assessments, satisfy documentation requirements and demonstrate compliance with applicable obligations are commonly assumed to remain capable of supporting transparency, oversight, accountability and regulatory control after deployment.

This assumption may not always hold.

Autonomous systems may continue operating in ways that remain formally compliant while simultaneously becoming progressively more difficult to observe, interpret, evaluate, audit or influence. In such situations, regulatory requirements may remain satisfied in a formal sense, yet the practical conditions required to support governance activities may gradually weaken over time.

This possibility introduces an important distinction.

Compliance describes whether regulatory requirements have been satisfied.

Governability describes whether systems remain capable of supporting the activities necessary to preserve transparency, accountability, oversight and regulatory continuity throughout runtime operation.

Although related, the two concepts are not equivalent.

A system may therefore remain compliant while exhibiting declining governability.

This paper refers to this phenomenon as the **Governability Gap**.

The Governability Gap describes situations in which systems continue to satisfy formal compliance requirements while simultaneously exhibiting insufficient governability during runtime operation. The concept highlights a potential discrepancy between regulatory status and operational reality. As autonomous systems become increasingly adaptive, distributed and operationally independent, such discrepancies may become increasingly important.

Building upon previous work on Regulatory Continuity, Continuous Governability and Governability by Design, this paper argues that the long-term challenge of autonomous systems

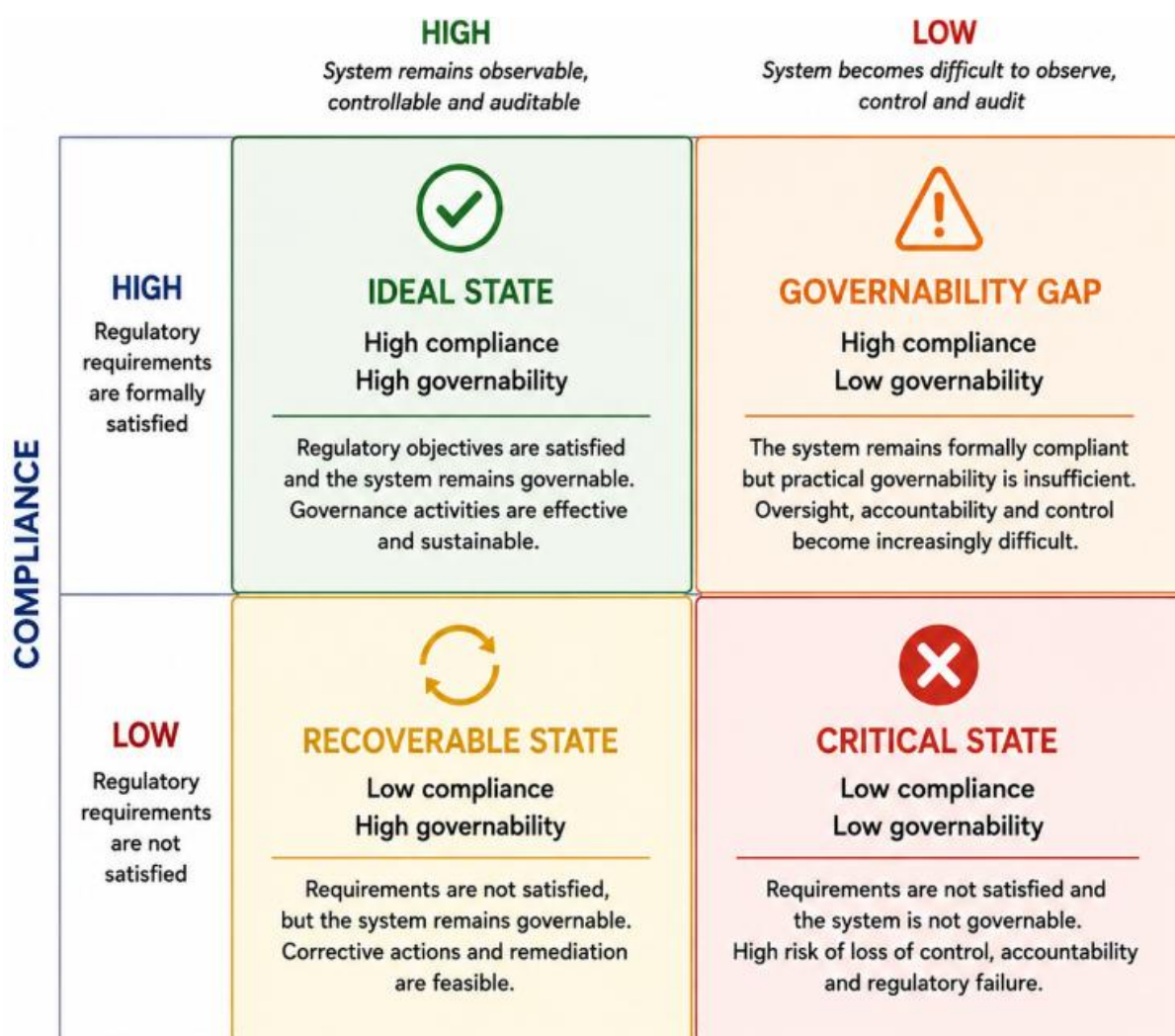
may not be limited to achieving compliance. Rather, the challenge may increasingly involve preserving the governability required to sustain compliance-relevant activities over time.

The paper further proposes that the Governability Gap may function as a leading indicator of future compliance degradation. As governability decreases, the ability to maintain transparency, accountability, oversight and risk management may progressively weaken, increasing the likelihood that regulatory objectives become difficult to preserve throughout continuous runtime operation.

Understanding, identifying and addressing the Governability Gap may therefore become increasingly important for future assurance frameworks, certification approaches and regulatory architectures under the EU AI Act.

Figure 1

### Compliance and Governability Are Not Equivalent



## **2. Compliance and Governability: A False Equivalence**

### **2.1 The Assumption of Equivalence**

Regulatory frameworks are generally designed to ensure that technological systems satisfy specific objectives related to safety, accountability, transparency, oversight and risk management. Compliance assessments, conformity procedures and certification processes serve as mechanisms for determining whether such objectives have been adequately addressed.

Within many regulatory discussions, compliance is frequently treated as evidence that governance mechanisms remain effective.

As a result, a common assumption emerges:

Systems that satisfy regulatory requirements are often presumed to remain sufficiently governable throughout operation.

This assumption appears intuitively reasonable.

If transparency requirements have been implemented, transparency is expected to remain available.

If accountability mechanisms exist, accountability is expected to remain achievable.

If human oversight procedures have been established, oversight is expected to remain meaningful.

Consequently, compliance and governability are often treated as closely aligned concepts.

However, compliance and governability address fundamentally different questions.

Compliance asks:

Have regulatory requirements been satisfied?

Governability asks:

Does the system remain capable of supporting governance-relevant activities throughout operation?

Although related, the two questions are not equivalent.

### **2.2 Compliance as an Evaluative Status**

Compliance represents an evaluative status.

It reflects the outcome of an assessment against a defined set of requirements, obligations or standards.

Compliance therefore answers whether a system conforms to applicable expectations at the time such evaluations are performed.

Certification, auditing, conformity assessment and regulatory review processes all operate primarily within this paradigm.

Under this perspective, compliance functions as a determination regarding the relationship between a system and a set of regulatory criteria.

Importantly, compliance itself does not necessarily guarantee that the conditions supporting compliance remain stable throughout future operation.

A system may satisfy requirements at one point in time while subsequently operating under changing circumstances, evolving environments or increasingly complex interactions.

Consequently, compliance should not automatically be interpreted as evidence that governance-relevant capabilities will remain equally effective throughout extended runtime operation.

## **2.3 Governability as an Operational Capability**

Governability differs fundamentally from compliance.

Rather than representing an evaluative status, governability describes an operational capability.

Specifically, governability reflects the extent to which a system remains capable of supporting observation, traceability, accountability, oversight, intervention and verification throughout runtime operation.

Governability therefore concerns the practical conditions that enable governance activities to remain effective.

This distinction is important.

Compliance may be established through evaluation.

Governability must be sustained through operation.

Compliance may be confirmed through certification.

Governability must remain continuously achievable.

Compliance may exist without active use.

Governability becomes relevant whenever governance activities are required.

From this perspective, governability functions as an enabling condition that allows compliance-related activities to remain operationally meaningful after deployment.

It is important to distinguish governability from controllability.

Controllability refers primarily to the ability to influence or constrain system behavior.

Governability encompasses a broader set of capabilities including observability, traceability, auditability, accountability and controllability.

Controllability may therefore be understood as one component of governability rather than an equivalent concept.

This distinction becomes increasingly important as autonomous systems evolve beyond traditional control-oriented paradigms toward complex socio-technical ecosystems requiring multiple governance-relevant capabilities simultaneously.

## **2.4 Divergence Between Compliance and Governability**

Because compliance and governability represent different concepts, they may evolve differently over time.

A system may remain compliant while simultaneously experiencing reductions in observability, traceability, auditability or controllability.

Similarly, increasing operational complexity may gradually reduce the practical effectiveness of governance mechanisms without immediately affecting formal compliance status.

Such divergence may emerge gradually rather than abruptly.

Transparency may remain available but become increasingly difficult to interpret.

Accountability records may continue to exist but become progressively harder to reconstruct.

Oversight mechanisms may remain formally present while becoming less effective in practice.

In such situations, regulatory requirements may remain satisfied while governability progressively deteriorates.

This observation suggests that compliance and governability should not be viewed as interchangeable concepts.

Rather, they should be understood as distinct dimensions that may strengthen, weaken or evolve independently.

## **2.5 The Consequences of False Equivalence**

Treating compliance and governability as equivalent may create a misleading perception of regulatory assurance.

If compliance is assumed to guarantee governability, gradual reductions in governability may remain undetected until more significant operational, accountability or oversight challenges emerge.

As a result, governance degradation may occur without corresponding indications of compliance failure.

This possibility is particularly relevant for autonomous systems operating across extended lifecycles characterized by adaptation, environmental change and distributed interactions.

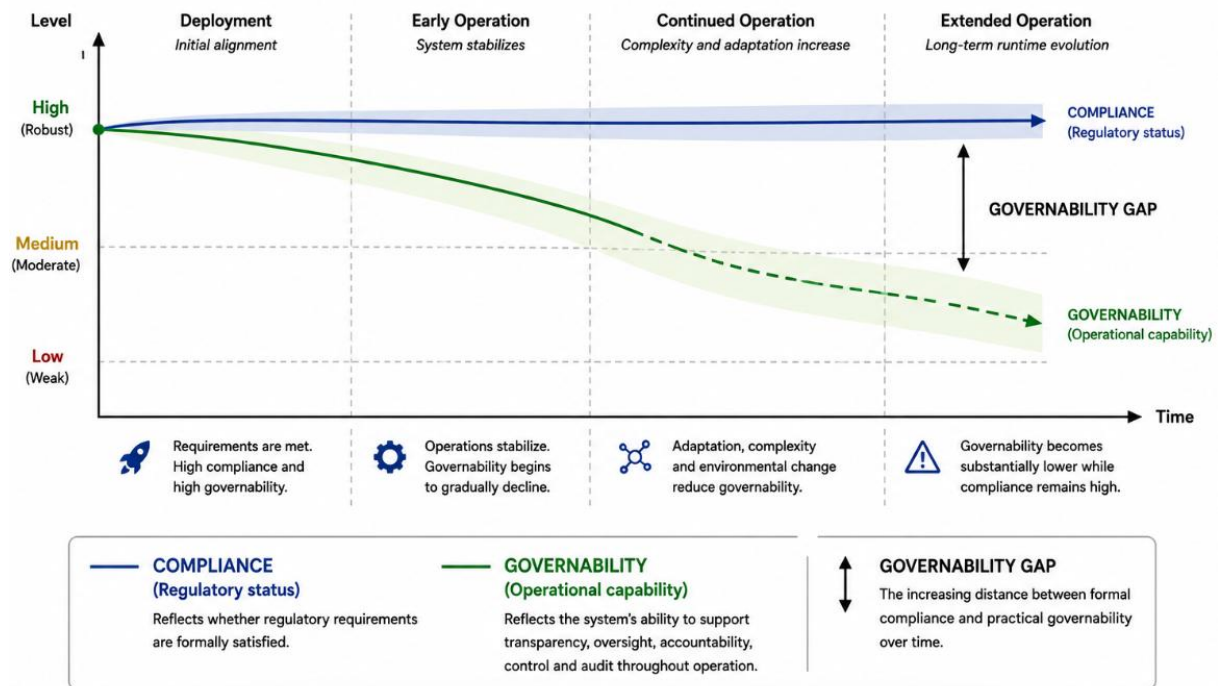
Under such conditions, maintaining governability may become increasingly difficult even when compliance obligations continue to be formally satisfied.

Recognizing the distinction between compliance and governability therefore represents a prerequisite for understanding the broader challenges associated with regulatory continuity.

The next section introduces the concept of the Governability Gap as a framework for describing situations in which compliance and governability diverge during runtime operation.

**Figure 2**

### Compliance and Governability Follow Different Trajectories



## 3. Defining the Governability Gap

### 3.1 Introducing the Governability Gap

The distinction between compliance and governability suggests the possibility of a previously underexplored challenge within autonomous systems governance.

If compliance and governability represent different concepts, then situations may emerge in which the two no longer evolve together.

A system may continue to satisfy regulatory requirements while simultaneously exhibiting declining governability during runtime operation.

This paper refers to such situations as the **Governability Gap**.

The Governability Gap describes the discrepancy between a system's formal compliance status and its practical governability during operation.



More specifically, the Governability Gap emerges when systems continue to satisfy compliance obligations while progressively losing the capabilities required to support governance-relevant activities such as observation, accountability, oversight, intervention and verification.

The concept highlights a potential divergence between regulatory status and operational reality.

While compliance may remain formally intact, governability may gradually deteriorate.

Understanding this divergence is essential because governance mechanisms ultimately depend upon governability capabilities in order to remain operationally effective.

### **3.2 Formal Definition**

For the purposes of this paper, the Governability Gap is defined as:

The discrepancy between formal compliance and the practical capacity of a system to support governance-relevant activities throughout runtime operation.

Under this definition, the Governability Gap does not necessarily imply non-compliance.

Nor does it imply regulatory failure.

Instead, it describes situations in which the practical conditions required to sustain transparency, accountability, oversight, auditability and risk management progressively weaken despite the continued satisfaction of compliance requirements.

The concept therefore focuses on capability degradation rather than regulatory violation.

This distinction is important because governance challenges may emerge long before formal compliance failures become visible.

### **3.3 Governability Gap as a Dynamic Phenomenon**

The Governability Gap should not be understood as a static condition.

Rather, it represents a dynamic phenomenon that may evolve gradually throughout a system lifecycle.

At deployment, compliance and governability may be closely aligned.

Over time, however, increasing complexity, adaptation, environmental change and operational evolution may influence governability in ways not immediately reflected by compliance status.

Consequently, the Governability Gap may expand, contract or fluctuate throughout operation.

The existence of such dynamics suggests that governability cannot be fully understood through point-in-time assessments alone.

Instead, governability may require continuous consideration throughout runtime operation.

This observation directly supports the broader concept of Regulatory Continuity introduced in previous work.



### **3.4 Compliance Without Governability**

One of the most important implications of the Governability Gap is the recognition that compliance and governability are not mutually dependent.

Compliance may exist without strong governability.

A system may continue to satisfy documentation requirements.

Logging mechanisms may remain operational.

Formal oversight procedures may remain in place.

Regulatory obligations may continue to be fulfilled.

Yet the practical ability to understand, interpret, reconstruct or influence system behavior may progressively weaken.

In such situations, governance activities become increasingly difficult despite the continued presence of compliance mechanisms.

The challenge therefore does not arise because regulatory requirements are absent.

Rather, it arises because the governability required to support those requirements has deteriorated.

This distinction forms the conceptual foundation of the Governability Gap.

### **3.5 The Governability Gap as a Leading Indicator**

The significance of the Governability Gap extends beyond governance itself.

The Governability Gap may also function as a leading indicator of future compliance degradation.

As governability decreases, the ability to sustain transparency, accountability, oversight and risk management may progressively weaken.

Initially, compliance may remain unaffected.

However, over time, continued reductions in governability may increase the likelihood that regulatory objectives become difficult to preserve.

The Governability Gap therefore provides an early warning perspective.

Rather than focusing exclusively on whether compliance failures have already occurred, attention shifts toward identifying conditions that may increase the probability of future compliance deterioration.

From this perspective, governability becomes relevant not only for governance but also for proactive regulatory assurance.

Consider an illustrative example involving an autonomous vehicle fleet.

At deployment, the fleet satisfies applicable regulatory requirements concerning documentation, logging, oversight procedures and risk management.

Over time, however, fleet behavior evolves through operational adaptation, changing traffic environments and increasingly complex coordination patterns.

Documentation remains available and compliance obligations remain formally satisfied.

Yet reconstructing specific operational decisions, understanding system-wide behavior and exercising meaningful oversight become progressively more difficult.

In such a situation, compliance may remain unchanged while governability declines.

The resulting divergence illustrates the emergence of a Governability Gap.

### **3.6 Why the Governability Gap Matters**

The Governability Gap matters because autonomous systems increasingly operate within environments characterized by continuous change.

Future autonomous systems may interact with evolving environments, changing objectives, distributed infrastructures and adaptive operational contexts.

Under such conditions, preserving governability may become progressively more difficult.

At the same time, regulatory objectives concerning accountability, transparency, oversight and risk management remain dependent upon the continued availability of governability capabilities.

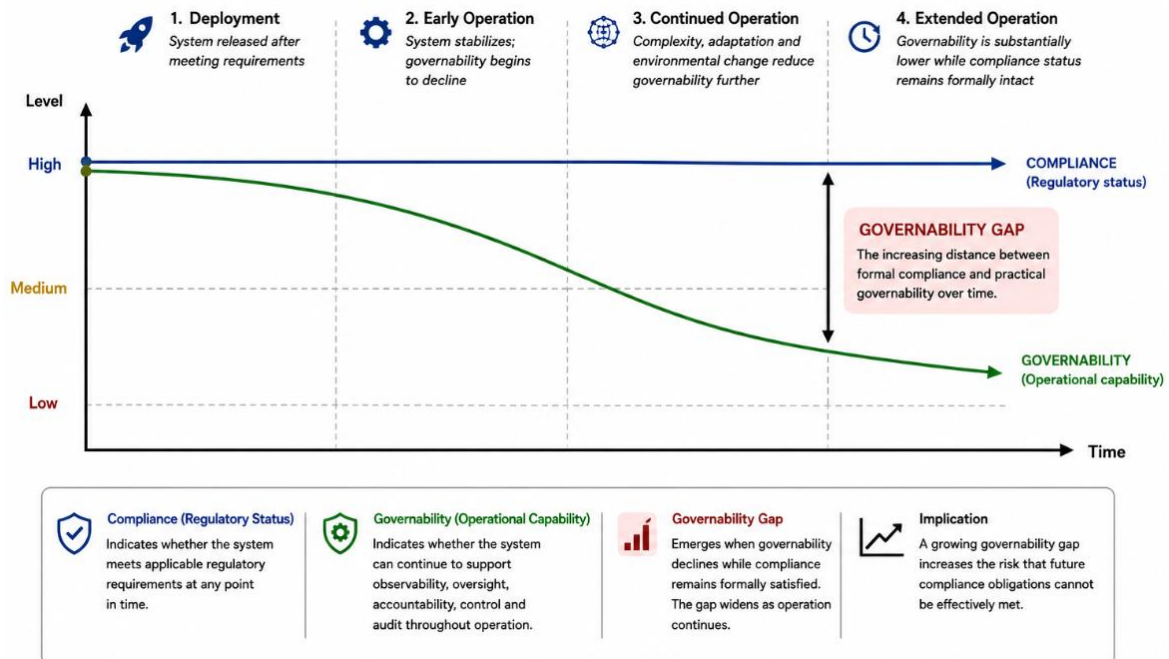
Consequently, the long-term effectiveness of governance frameworks may depend not only upon compliance requirements themselves, but also upon the extent to which systems remain governable throughout operation.

The Governability Gap therefore represents more than a governance concern.

It represents a potential challenge for maintaining regulatory continuity within increasingly autonomous technological ecosystems.

**Figure 3**

## Emergence of the Governability Gap



## 4. Sources of Governability Degradation

### 4.1 Governability Does Not Necessarily Remain Stable

Traditional compliance approaches often assume that governance-relevant capabilities remain relatively stable following deployment.

Under this assumption, systems that satisfy transparency, accountability, oversight and risk management requirements during certification are expected to continue supporting these objectives throughout operation.

Autonomous systems increasingly challenge this assumption.

Unlike static systems, autonomous systems frequently operate within changing environments, interact with evolving conditions and participate in dynamic operational ecosystems.

As a result, governability should not be assumed to remain constant over time.

Rather, governability may strengthen, weaken or evolve throughout runtime operation.

Understanding the mechanisms that contribute to governability degradation is therefore essential for understanding how the Governability Gap emerges.

## 4.2 Increasing Operational Complexity

One of the most significant sources of governability degradation is increasing operational complexity.

As autonomous systems become more sophisticated, the number of interactions, dependencies and operational pathways often grows substantially.

Additional sensors, models, decision processes, interfaces and external interactions may increase system functionality while simultaneously reducing the ability of operators, auditors and regulators to understand overall system behavior.

Complexity does not necessarily reduce compliance.

However, it may reduce transparency, traceability and interpretability.

Consequently, increasing complexity may contribute directly to reductions in governability.

## 4.3 Runtime Adaptation

Autonomous systems increasingly adapt to changing operational conditions.

Adaptation may involve modifications to behavioral strategies, decision priorities, coordination patterns or environmental responses.

Such adaptation can improve operational performance.

However, adaptation may also complicate governance activities.

Behavioral changes that occur gradually over time may remain difficult to identify, evaluate or interpret.

As adaptation increases, maintaining visibility into how and why systems behave in particular ways may become increasingly challenging.

Runtime adaptation therefore represents a potential source of governability degradation even when adaptation itself remains beneficial.

## 4.4 Distributed Coordination

Many future autonomous systems will not operate in isolation.

Instead, they may participate in fleets, networks, ecosystems and distributed infrastructures involving interactions among multiple autonomous entities.

Distributed coordination introduces additional governance challenges.

Responsibility may become more difficult to attribute.

Decision pathways may become increasingly distributed.

Operational outcomes may emerge from interactions among multiple systems rather than individual system actions.

As coordination complexity increases, maintaining accountability, oversight and traceability may become progressively more difficult.

Distributed coordination therefore represents another significant source of governability degradation.

## **4.5 Environmental Evolution**

Governability may also be influenced by changes occurring outside the system itself.

Operational environments frequently evolve over time.

New stakeholders emerge.

User behaviors change.

Infrastructure evolves.

Operational objectives shift.

Regulatory expectations develop.

These changes may affect the relationship between system behavior and governance mechanisms.

Capabilities that once supported effective oversight may gradually become less effective under new conditions.

Environmental evolution therefore contributes to governability degradation by altering the context within which governance activities occur.

## **4.6 Emergent Behavior**

Autonomous systems may exhibit behaviors that are not easily predictable from individual system components alone.

Such emergent behaviors can arise through interactions among multiple subsystems, agents or environmental conditions.

Emergence does not necessarily imply malfunction.

However, emergent behavior may complicate governance activities.

Unexpected interactions can reduce predictability, challenge accountability and increase the difficulty of reconstructing operational events.

As emergent phenomena become more prominent, maintaining governability may require increasingly sophisticated approaches to observation and oversight.

## 4.7 Governance Capability Erosion

A particularly important source of governability degradation involves the gradual erosion of governance capabilities themselves.

Observability may decline.

Traceability may become incomplete.

Auditability may weaken.

Accountability relationships may become less clear.

Controllability may become more difficult to exercise.

Importantly, such erosion may occur without immediate compliance consequences.

Compliance mechanisms may remain formally present even as their practical effectiveness diminishes.

This distinction highlights why governability degradation can remain difficult to detect through compliance-focused assessments alone.

## 4.8 Governability Degradation as a Systemic Process

The sources described above should not be viewed as isolated phenomena.

In practice, they frequently interact.

Increasing complexity may amplify adaptation challenges.

Adaptation may influence accountability.

Distributed coordination may increase emergence.

Environmental evolution may reduce the effectiveness of oversight mechanisms.

As these factors interact, governability degradation may become a systemic process rather than a single identifiable event.

This observation suggests that the Governability Gap should not be understood as the result of individual failures.

Instead, it may emerge gradually through the cumulative effects of multiple interacting forces operating throughout system lifecycles.

**Figure 4**

## Sources of Governability Degradation



## 5. The Governability Gap under the EU AI Act

### 5.1 Transparency Requirements and the Hidden Governability Dependency

The EU AI Act places significant emphasis on transparency obligations for high-risk AI systems, particularly through requirements concerning technical documentation (Article 11), logging capabilities (Article 12) and transparency-related information obligations (Article 13).

Providers are expected to maintain technical documentation, ensure traceability, provide meaningful information to deployers, and support regulatory oversight. These requirements are intended to improve visibility into system behavior and to facilitate accountability throughout the lifecycle of an AI system.

However, transparency and governability are not equivalent concepts.

A system may remain fully transparent while simultaneously becoming increasingly difficult to govern. Documentation may accurately describe a system's architecture, intended functionality, operational limits, and risk controls, yet provide little assurance that the system remains controllable during runtime operation.

The distinction becomes particularly relevant as autonomous systems increase in complexity, autonomy, and operational duration. Transparency primarily concerns the availability of



information. Governability concerns the ability to influence, constrain, redirect, or terminate system behavior when necessary.

This creates a hidden dependency within transparency requirements. Information about a system only becomes operationally useful if the system remains governable. Without effective mechanisms for intervention and control, transparency may reveal the existence of problematic behavior without providing the capability to prevent or correct it.

The Governability Gap therefore introduces a critical limitation to transparency-based regulatory approaches. Transparency can support oversight, but oversight alone does not guarantee control. A system may remain fully observable while progressively losing governability.

Consequently, transparency should not be understood as an independent assurance mechanism. Rather, its practical effectiveness depends upon the existence of sufficient governability capabilities that allow observed risks, deviations, or failures to be addressed during runtime operation.

This dependency suggests that future assurance frameworks may need to evaluate not only what can be observed about autonomous systems, but also whether observed conditions can be meaningfully governed once the system is deployed.

## **5.2 Transparency and Observability Degradation**

Transparency is frequently viewed as a cornerstone of trustworthy AI governance.

However, transparency depends upon the ability to obtain meaningful insight into system behavior.

As operational complexity increases, maintaining such visibility may become increasingly difficult.

Information may remain available.

Logs may continue to be generated.

Documentation may continue to exist.

Yet the practical ability to understand system behavior may gradually weaken.

In such situations, transparency remains formally present while becoming progressively less meaningful in practice.

This represents a potential manifestation of the Governability Gap.

## **5.3 Human Oversight and Controllability Degradation**

Article 14 of the EU AI Act places significant emphasis on human oversight capabilities for high-risk AI systems.

Meaningful oversight, however, requires more than the existence of oversight procedures.

Oversight must remain operationally feasible.

Human operators must retain the ability to observe, understand and influence system behavior when necessary.

As systems become increasingly adaptive, distributed and operationally complex, maintaining such capabilities may become more difficult.

Formal oversight mechanisms may continue to exist.

Yet the practical ability to exercise effective oversight may progressively decline.

This distinction illustrates how governability degradation may influence oversight effectiveness without necessarily producing immediate compliance failures.

## **5.4 Accountability and Traceability Degradation**

Accountability depends upon the ability to reconstruct events, understand decision pathways and establish relationships between actions and outcomes.

Traceability therefore represents a critical governability capability.

As systems become increasingly distributed and adaptive, maintaining comprehensive traceability may become progressively more challenging.

Records may remain available.

Logging requirements may remain satisfied.

However, reconstructing operational behavior may become increasingly difficult due to complexity, distributed interactions and emergent effects.

The result may be accountability mechanisms that remain formally present while becoming increasingly difficult to apply in practice.

As a consequence, accountability may increasingly become a function of governability.

Without sufficient traceability and reconstructability, the practical ability to assign responsibility may progressively weaken even when accountability mechanisms remain formally established.

## **5.5 Risk Management and Predictability Degradation**

Risk management constitutes a central requirement under Article 9 of the EU AI Act.

Predictability therefore plays a central role in effective governance.

Autonomous systems operating within evolving environments may gradually become more difficult to anticipate.

Behavioral adaptation, environmental change and distributed interactions may introduce increasing uncertainty regarding future operational outcomes.

Although risk management processes may continue to exist, declining predictability may reduce their practical effectiveness.

This represents another pathway through which governability degradation may influence regulatory objectives.

## 5.6 Post-Market Monitoring and Adaptation Visibility

The EU AI Act introduces post-market monitoring obligations through Article 72, recognizing the importance of observing system behavior after deployment.

Such monitoring assumes that relevant changes in system behavior remain identifiable and assessable throughout operation.

However, effective monitoring depends upon adaptation visibility.

If behavioral changes become increasingly difficult to identify or interpret, monitoring activities may become progressively less effective despite the continued existence of monitoring mechanisms.

Consequently, adaptation visibility may represent a critical governability capability supporting long-term regulatory continuity.

## 5.7 The Hidden Governability Dependency

Collectively, these observations suggest a broader conclusion.

Many regulatory objectives appear to depend upon governability capabilities even when governability itself is not explicitly identified as a regulatory requirement.

This relationship may be described as a Hidden Governability Dependency.

The concept extends the previously proposed Hidden Governability Assumption by emphasizing the operational dependence of regulatory objectives upon governability capabilities.

Under this perspective, governability becomes more than a governance concern.

It becomes an enabling condition supporting the practical achievement of multiple regulatory objectives simultaneously.

## 5.8 Implications for Regulatory Continuity

The significance of the Governability Gap ultimately extends beyond individual compliance requirements.

As autonomous systems become increasingly adaptive and operationally independent, preserving governability may become essential for maintaining regulatory continuity itself.

The challenge is therefore not limited to demonstrating compliance.

The challenge increasingly involves preserving the conditions that allow compliance-related activities to remain meaningful throughout runtime operation.

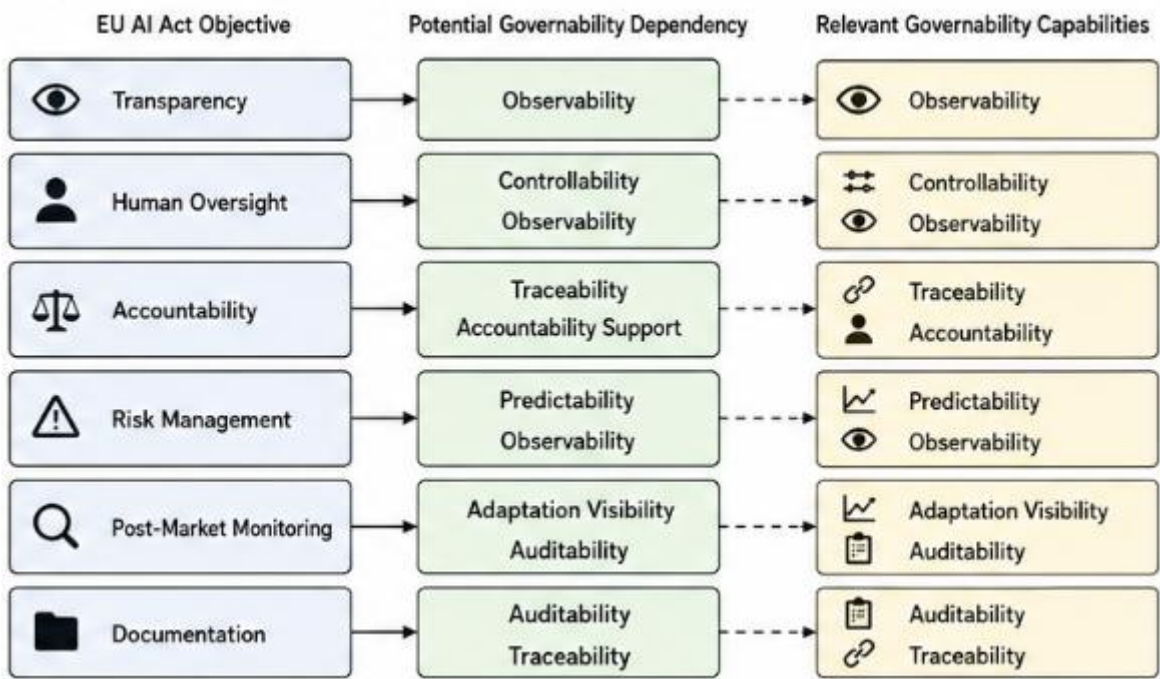
From this perspective, the Governability Gap represents a potential obstacle to long-term regulatory effectiveness.

Understanding and addressing this challenge may become increasingly important as autonomous systems continue to evolve in scale, complexity and autonomy.

This observation suggests that governability may function as a hidden enabling layer beneath multiple regulatory objectives of the EU AI Act.

Figure 5

EU AI Act Objectives and Potential Governability Dependencies



While regulatory requirements explicitly address transparency, accountability, human oversight, risk management and post-market monitoring, the practical achievement of these objectives may depend upon the continued availability of underlying governability capabilities.

The challenge may therefore extend beyond compliance itself toward preserving the operational conditions that allow compliance-related activities to remain achievable throughout runtime operation.

### 5.9 Governability as a Precondition for Regulatory Objectives

A broader interpretation of the preceding analysis suggests that governability may function as a foundational precondition underlying multiple regulatory objectives of the EU AI Act.

Transparency requires the continued ability to observe and interpret system behavior.

Human oversight requires the continued ability to influence or constrain system operation.

Accountability requires the continued ability to reconstruct operational events and decision pathways.

Risk management requires the continued ability to evaluate evolving operational conditions and emerging risks.

Post-market monitoring requires the continued ability to identify, assess and interpret behavioral changes throughout operation.

In each case, regulatory objectives appear to depend upon the existence of underlying governability capabilities.

This observation does not imply that governability should replace existing regulatory requirements.

Rather, it suggests that governability may represent a higher-order system property that enables regulatory objectives to remain operationally achievable throughout runtime operation.

In this sense, governability may be understood as the operational substrate upon which multiple regulatory objectives depend.

From this perspective, the Governability Gap becomes particularly significant.

As governability decreases, the practical feasibility of achieving regulatory objectives may progressively weaken even when compliance requirements remain formally satisfied.

The challenge therefore extends beyond demonstrating compliance at a specific point in time.

The challenge increasingly involves preserving the governability required to sustain compliance-relevant capabilities throughout the operational lifecycle of autonomous systems.

This perspective reinforces the central argument of the paper: future regulatory effectiveness may depend not only upon compliance mechanisms themselves, but also upon the extent to which systems remain governable after deployment.

## **6. Governability as a Leading Indicator of Compliance Degradation**

### **6.1 Beyond Compliance Failure**

Traditional regulatory approaches primarily focus on identifying situations in which compliance failures have already occurred.

Audits, conformity assessments, investigations and enforcement activities are typically triggered by the detection of non-compliance, regulatory violations or evidence that applicable requirements are no longer being satisfied.

While such approaches remain important, they are inherently reactive.

They identify problems after governance-relevant capabilities have already deteriorated sufficiently to affect compliance outcomes.

The Governability Gap introduces a different perspective.

Rather than focusing exclusively on compliance failures, attention shifts toward identifying conditions that may increase the likelihood of future compliance degradation.

Under this perspective, governability becomes relevant not because compliance has already failed, but because declining governability may create circumstances under which compliance becomes increasingly difficult to sustain.

The distinction is significant.

Compliance failure represents an outcome.

Governability degradation represents a process.

Understanding this process may provide opportunities to identify emerging governance challenges before formal compliance failures become visible.

Consequently, the Governability Gap may offer a valuable framework for moving from reactive regulatory assessment toward more proactive forms of regulatory assurance.

## **6.2 Governability Degradation Precedes Compliance Degradation**

A central argument of this paper is that reductions in governability may frequently occur before observable compliance failures emerge.

This sequence is consistent with the distinction established throughout the paper.

Governability reflects the operational capability required to support transparency, accountability, oversight, auditability and risk management.

Compliance reflects the formal status associated with these objectives.

Because compliance mechanisms depend upon underlying governability capabilities, degradation of governability may occur before compliance itself becomes visibly affected.

Observability may weaken before transparency obligations become difficult to satisfy.

Controllability may decline before oversight requirements become ineffective.

Traceability may deteriorate before accountability investigations encounter significant limitations.

Predictability may decrease before risk management processes become insufficient.

Consequently, governability degradation may function as an early-stage phenomenon that precedes more visible manifestations of regulatory deterioration.

This observation suggests that governability metrics may provide earlier indications of emerging governance challenges than compliance assessments alone.

## **6.3 The Progressive Expansion of the Governability Gap**

The Governability Gap should not be understood as a binary condition.

Rather, the gap may expand gradually over time.

Initially, compliance and governability may remain closely aligned.

As operational complexity increases, adaptation accumulates and environments evolve, governability may begin to decline.

At first, the reduction may have little practical impact.

Governance activities remain feasible.

Oversight remains effective.

Accountability remains achievable.

Transparency remains meaningful.

Over time, however, continued reductions in governability may progressively weaken these capabilities.

The resulting gap between compliance status and practical governability widens.

Eventually, the gap may reach a point at which governance activities become increasingly difficult to perform despite the continued existence of formal compliance mechanisms.

This gradual progression highlights why the Governability Gap may remain difficult to identify through conventional compliance assessments.

The challenge emerges incrementally rather than through abrupt failure.

## **6.4 Governability Metrics as Early Warning Signals**

If governability degradation precedes compliance degradation, then measuring governability may provide valuable early warning signals.

Future assurance frameworks may therefore benefit from assessing governance-relevant capabilities directly.

Examples may include:

- Observability effectiveness
- Traceability completeness
- Auditability performance
- Accountability reconstruction capability
- Controllability effectiveness
- Adaptation visibility
- Predictability stability
- Oversight responsiveness

Such indicators would not replace compliance assessments.

Instead, they would complement existing compliance approaches by providing visibility into the underlying capabilities that support regulatory objectives.



From this perspective, governability assessment becomes analogous to monitoring structural integrity rather than waiting for structural failure.

The objective is not merely to identify violations after they occur, but to detect conditions that increase the probability of future governance breakdown.

Future work may ultimately enable the development of Governability Indicators analogous to safety indicators, resilience indicators or cybersecurity metrics currently used within other assurance disciplines.

Such indicators could provide quantitative visibility into the evolving governance capacity of autonomous systems throughout operation.

## 6.5 From Compliance Assessment to Governability Assessment

The emergence of the Governability Gap suggests a potential evolution in assurance methodologies.

Traditional compliance frameworks primarily evaluate whether regulatory requirements have been satisfied.

Future assurance frameworks may increasingly need to evaluate whether systems remain capable of sustaining those requirements throughout operation.

This distinction introduces the possibility of governability assessment as a complementary assurance activity.

### **Compliance assessment asks:**

*Are regulatory requirements satisfied?*

### **Governability assessment asks:**

*Can the system continue supporting those requirements throughout runtime operation?*

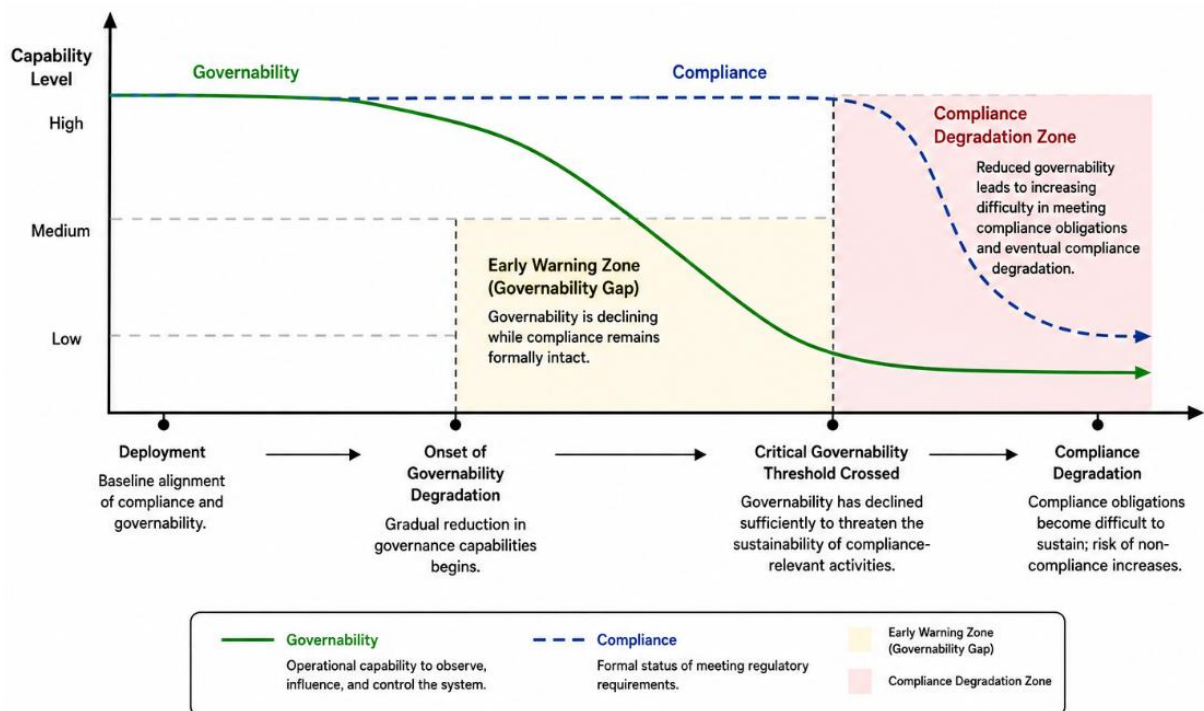
The difference appears subtle but may become increasingly important as autonomous systems evolve toward greater autonomy, adaptation and operational independence.

Under such conditions, maintaining governability may become as important as demonstrating compliance itself.

From this perspective, the Governability Gap functions not only as a governance concept but also as a framework for anticipating future compliance challenges before they become visible through conventional regulatory mechanisms.

**Figure 6**

## **Governability Degradation as a Leading Indicator of Compliance Degradation**



## **7. Implications for Future Assurance and Certification**

### **7.1 The Limits of Static Compliance Assessment**

Contemporary assurance and certification frameworks are largely based on point-in-time evaluations.

Conformity assessments, audits, certification procedures and regulatory reviews typically examine whether a system satisfies applicable requirements at the moment of evaluation.

This approach has proven effective for many traditional technologies whose operational characteristics remain relatively stable following deployment.

Autonomous systems introduce new challenges.

As systems become increasingly adaptive, distributed and operationally dynamic, conditions relevant to governance may evolve continuously throughout runtime operation.

Under such circumstances, point-in-time assessments may provide only a partial view of long-term governance capability.

A system may satisfy all applicable requirements during certification while subsequently experiencing gradual reductions in observability, traceability, controllability or accountability.

The existence of the Governability Gap suggests that static compliance assessments may therefore be insufficient for understanding long-term regulatory effectiveness.

The challenge extends beyond determining whether systems are compliant at deployment.

The challenge increasingly involves determining whether systems remain governable throughout operation.

## 7.2 Toward Continuous Assurance

The concept of the Governability Gap supports a broader shift from static assurance toward continuous assurance.

Continuous assurance does not imply continuous recertification.

Rather, it reflects the recognition that governance-relevant capabilities may require ongoing evaluation throughout runtime operation.

Under this perspective, assurance activities expand beyond initial compliance verification and incorporate mechanisms capable of identifying emerging reductions in governability.

Examples may include:

- Continuous observability assessment
- Runtime traceability verification
- Oversight effectiveness evaluation
- Accountability reconstruction testing
- Adaptation visibility monitoring
- Predictability assessment

Such approaches focus on the operational sustainability of governance capabilities rather than solely on initial compliance status.

The objective is not merely to confirm that governance mechanisms exist, but to verify that they remain effective throughout system lifecycles.

Under such a perspective, certification may gradually evolve from a primarily static assessment of compliance toward an evaluation of sustained governability.

The question would no longer be limited to whether a system satisfies requirements at the time of certification, but whether it remains capable of sustaining those requirements throughout operation.

## 7.3 Governability-Oriented Certification

The Governability Gap also raises important questions regarding the future evolution of certification frameworks.

Traditional certification primarily evaluates whether systems satisfy predefined requirements.

Future certification approaches may additionally consider whether systems possess sufficient governability characteristics to sustain regulatory objectives throughout operation.

This does not necessarily require entirely new certification regimes.

Instead, existing certification frameworks may gradually incorporate governability-oriented evaluation criteria.

Examples could include assessments of:

- Runtime observability capabilities
- Traceability persistence
- Oversight sustainability
- Accountability resilience
- Adaptation transparency
- Intervention effectiveness
- Governance capability robustness

Such criteria would focus not only on compliance outcomes but also on the underlying capabilities required to preserve those outcomes over time.

Certification would therefore move beyond demonstrating compliance toward demonstrating sustainable governability.

## **7.4 Governability by Design**

The Governability Gap reinforces the importance of architectural approaches to governance.

If governability can degrade throughout operation, then governability cannot be treated solely as a procedural or organizational concern.

Instead, governability may increasingly depend upon architectural considerations.

This observation aligns with the broader concept of Governability by Design introduced in previous work.

Governability by Design argues that governance-relevant capabilities should be considered during system design rather than added as external controls after deployment.

Observability, traceability, accountability, controllability and auditability may therefore be understood as architectural properties that influence the long-term sustainability of governance activities.

Under this perspective, reducing the Governability Gap becomes partially an architectural challenge.

The objective is not simply to achieve compliance but to design systems that remain governable throughout continuous runtime operation.

## 7.5 Regulatory Continuity and Long-Term Governance

The Governability Gap ultimately highlights a broader challenge concerning regulatory continuity.

Most regulatory objectives assume that governance mechanisms remain effective after deployment.

However, the increasing autonomy and operational complexity of future systems may make such assumptions progressively more difficult to sustain.

Maintaining regulatory continuity may therefore require greater attention to the long-term preservation of governance capabilities.

Transparency must remain meaningful.

Accountability must remain achievable.

Oversight must remain operationally feasible.

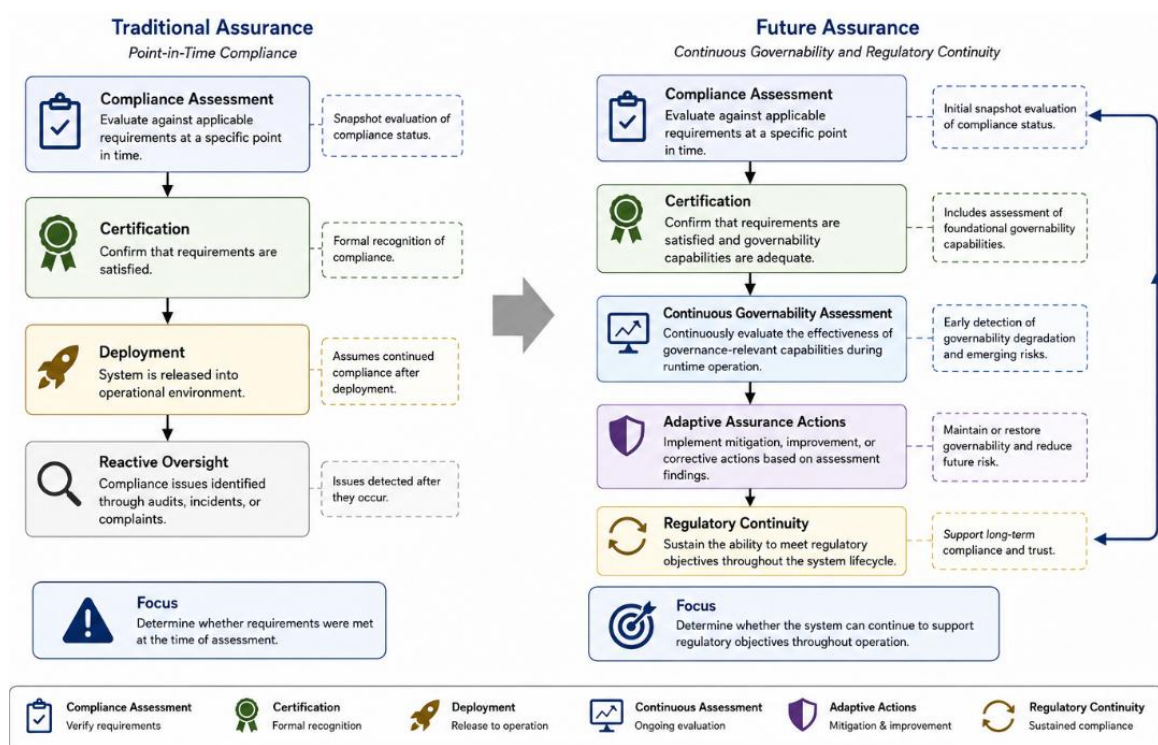
Risk management must remain effective. These objectives depend upon governability.

Consequently, preserving governability may become a central requirement for maintaining regulatory continuity within increasingly autonomous technological ecosystems.

From this perspective, the Governability Gap represents not merely a governance concern but a broader challenge for the future evolution of assurance, certification and regulatory architectures.

Figure 7

### Evolution of Assurance Frameworks



## 8. Conclusion

The EU AI Act represents one of the most comprehensive regulatory efforts aimed at ensuring the safe, trustworthy and accountable deployment of artificial intelligence systems.

Its provisions concerning transparency, accountability, human oversight, risk management and post-market monitoring establish important foundations for governing increasingly autonomous technologies.

However, the growing autonomy, adaptability and operational complexity of future autonomous systems introduce challenges that extend beyond the traditional boundaries of compliance.

This paper has argued that compliance and governability represent distinct concepts.

Compliance describes whether regulatory requirements have been satisfied.

Governability describes whether systems remain capable of supporting the governance activities required to sustain those requirements throughout runtime operation.

Because the two concepts are not equivalent, situations may emerge in which systems remain formally compliant while simultaneously experiencing declining governability.

This paper introduced the concept of the Governability Gap to describe this discrepancy between regulatory status and practical governability.

The analysis identified multiple sources of governability degradation, including increasing operational complexity, runtime adaptation, distributed coordination, environmental evolution, emergent behavior and the erosion of governance capabilities themselves.

These factors may gradually weaken observability, traceability, controllability, accountability and auditability without necessarily producing immediate compliance failures.

The paper further proposed that the Governability Gap may function as a leading indicator of future compliance degradation.

As governability decreases, the practical ability to sustain transparency, oversight, accountability and risk management may progressively weaken.

Consequently, governability degradation may become visible before formal compliance failures emerge.

This perspective suggests that future assurance and certification approaches may benefit from complementing compliance assessment with governability assessment.

Evaluating whether systems remain capable of supporting governance activities throughout operation may become increasingly important as autonomous systems continue to evolve.

More broadly, the analysis suggests that many regulatory objectives of the EU AI Act depend upon underlying governability capabilities even when governability itself is not explicitly identified as a regulatory requirement.

Transparency depends upon observability.

Oversight depends upon controllability.

Accountability depends upon traceability.

Risk management depends upon predictability and visibility into system behavior.

The effectiveness of these objectives may therefore depend upon the extent to which systems remain governable after deployment.

The central implication is straightforward.

The long-term challenge of autonomous systems may not be limited to achieving compliance.

The challenge may increasingly involve preserving the governability required to sustain compliance throughout continuous runtime operation.

Understanding, measuring and maintaining governability may therefore become an essential component of future regulatory continuity.

As autonomous systems continue to expand across industrial, commercial and societal domains, the ability to remain governable may ultimately determine whether compliance can remain meaningful over time.

## **Future Research**

Future research may explore methods for measuring governability, developing governability metrics, identifying governability degradation patterns and designing architectures capable of sustaining governability throughout extended runtime operation.

Particular attention may be devoted to the relationship between governability and certification continuity, runtime assurance, autonomous system resilience and long-term regulatory effectiveness.

A broader research agenda may ultimately contribute to the emergence of a formal science of governability capable of supporting the governance of increasingly autonomous technological ecosystems.

More broadly, future research may investigate the relationship between governability and long-term regulatory sustainability.

A central question emerges: why do some autonomous systems remain governable throughout extended operational lifecycles while others progressively lose the capacity to support governance activities despite remaining formally compliant?

Addressing this question may contribute to the development of a broader science of regulatory sustainability for autonomous systems.

More fundamentally, future research may investigate whether governability itself can be formalized as a measurable system property.

Such work could contribute to the development of a broader science of governability capable of explaining why some autonomous systems preserve governance capacity throughout extended operational lifecycles while others experience progressive governability degradation despite remaining formally compliant.

The Governability Gap may therefore represent an initial conceptual foundation for a broader research field concerned with the long-term sustainability of governance in autonomous systems.



## References

- European Parliament and Council of the European Union. (2024). *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Official Journal of the European Union.
- European Commission. (2021). *Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. COM(2021) 206 final.
- European Commission High-Level Expert Group on Artificial Intelligence. (2019). *Ethics Guidelines for Trustworthy AI*. European Commission.
- Dignum, V. (2019). *Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way*. Springer.
- Floridi, L., & Cowls, J. (2019). A Unified Framework of Five Principles for AI in Society. *Harvard Data Science Review*, 1(1).
- Leslie, D. (2019). *Understanding Artificial Intelligence Ethics and Safety*. The Alan Turing Institute.
- Bryson, J. J. (2018). Patience Is Not a Virtue: The Design of Intelligent Systems and Systems of Ethics. *Ethics and Information Technology*, 20(1), 15–26.
- Mitchell, M. (2009). *Complexity: A Guided Tour*. Oxford University Press.
- Holland, J. H. (2014). *Complexity: A Very Short Introduction*. Oxford University Press.
- Simon, H. A. (1962). The Architecture of Complexity. *Proceedings of the American Philosophical Society*, 106(6), 467–482.
- Leveson, N. G. (2011). *Engineering a Safer World: Systems Thinking Applied to Safety*. MIT Press.
- Rasmussen, J. (1997). Risk Management in a Dynamic Society: A Modelling Problem. *Safety Science*, 27(2–3), 183–213.
- Hollnagel, E. (2014). *Safety-I and Safety-II: The Past and Future of Safety Management*. Ashgate.
- Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press.
- Zuboff, S. (2019). *The Age of Surveillance Capitalism*. PublicAffairs.
- Hildebrandt, M. (2020). *Law for Computer Scientists and Other Folk*. Oxford University Press.
- Blumer, A. (2026). *Continuous Governability for Autonomous Systems: Toward Persistent Governance Infrastructures for Autonomous Ecosystems*. Zenodo. <https://doi.org/10.5281/zenodo.20368587>
- Blumer, A. (2026). *The Economics of Governability: Why Autonomous Ecosystems May Require Persistent Governance Infrastructure*. Zenodo. <https://doi.org/10.5281/zenodo.20374895>
- Blumer, A. (2026). *Governability by Design: Architectural Requirements for Continuous Compliance under the EU AI Act*. Zenodo. <https://doi.org/10.5281/zenodo.20497153>
- Blumer, A. (2026). *From Compliance to Governability: The Emerging Infrastructure Logic of the EU AI Act*. Zenodo. <https://doi.org/10.5281/zenodo.20478361>

Blumer, A. (2026). *Governance Infrastructure for Autonomous Systems under the EU AI Act*. Zenodo. <https://doi.org/10.5281/zenodo.20346616>

Blumer, A. (2026). *The Predictability Challenge of Autonomous Systems: Implications for Governance, Assurance and Regulatory Continuity*. Zenodo. <https://doi.org/10.5281/zenodo.20451283>