International Journal of
Science, Architecture, Technology and Environment

Continuous Compliance: Turning Cyber Controls into Always-On, Verifiable Evidence

Ayomipo Alademehin [1*]

[1]*Lamar University*

[*]*Corresponding author- aalademehin@lamar.edu*

DOI: https://doi.org/10.63680/ijsate0226044.042

Abstract

Cybersecurity compliance is shifting from periodic, point-in-time assessments toward ongoing evidence and assurance expectations driven by cloud-native systems, DevSecOps practices, and expanding regulatory and contractual requirements. Yet the term "continuous compliance" remains conceptually ambiguous and inconsistently operationalized across cybersecurity, IT risk management, governance risk and compliance (GRC), and audit assurance communities. This fundamentals paper conceptualizes continuous compliance in Information Systems (IS) research using a multivocal review of standards, assurance guidance, and academic work. It introduces a core conceptual model consisting of seven interacting aspects: compliance obligations, risk appetite and governance, control design and implementation, evidence and telemetry, assurance actors and accountability, compliance automation infrastructure, and trust and transparency outcomes. The model is discussed through contemporary field examples (SOC 2 for cloud services, PCI DSS environments, and ISO/IEC 27001 programs) and results in a structured research agenda spanning design science research (DSR) and behavioral research.

Keywords: continuous compliance; cybersecurity governance; IT risk management; GRC; continuous control monitoring; audit evidence; compliance automation; policy-as-code.

1. Introduction

Information Systems increasingly operate in environments where software changes continuously, infrastructure is created and destroyed dynamically, and data moves across complex ecosystems of vendors, platforms, and jurisdictions. In this context, point-in-time compliance and annual audits are frequently misaligned with real operational risk. Misconfigurations can persist undetected while new code and infrastructure are deployed within hours.

At the same time, expectations of compliance continue to grow. Boards demand clearer cyber risk reporting, customers expect security assurance for vendors, insurers request security posture evidence, and regulators increasingly emphasize accountability. This has accelerated a shift toward continuous approaches: continuously verifying controls, continuously collecting evidence, and continuously reporting compliance

posture.

Despite its popularity, continuous compliance remains conceptually fragmented. In practice, it overlaps with continuous control monitoring (CCM), compliance automation, audit-ready evidence pipelines, continuous assurance, and policy-as-code. In research, adjacent work exists in DevSecOps, audit analytics, security metrics, governance, and enterprise risk management, yet there is limited agreement on what continuous compliance is, what components are essential, and how it changes trust and accountability relationships among control owners, auditors, customers, and regulators.

2. Background and related work

2.1 From periodic compliance to continuous expectations

Traditional security compliance has largely been periodic: annual audits, quarterly access reviews, monthly vulnerability scans, and periodic risk assessments. Modern cloud-native environments create faster control drift and higher change velocity, making retrospective evidence less useful for managing current risk.

2.2 Terminological ambiguity: monitoring, compliance, and assurance

Continuous compliance is often in conflict with related concepts. Continuous monitoring commonly refers to ongoing telemetry and awareness. Continuous control monitoring emphasizes ongoing evaluation of control effectiveness. Continuous assurance emphasizes more frequent testing and reporting to assurance stakeholders. Compliance automation focuses on tooling that maps control evidence sources and reduces manual audit preparation. These ideas overlap but are not identical.

2.3 Why conceptual structure needed in IS

From an IS perspective, continuous compliance is a socio-technical assurance mechanism shaped by governance, incentives, accountability, and evidence sufficiency expectations. Without shared conceptual structure, organizations risk investing in tools that produce noise rather than trustworthy evidence and outcomes.

3. Research approach and theoretical lens

3.1 Multivocal review and conceptual modeling

This paper integrates academic concepts with practitioner standards, assurance guidance, and industry artifacts to structure a practice-led domain. The goal is conceptual consolidation and model utility rather than exhaustive coverage.

3.2 Agency theory lens

Agency theory explains assurance needs when stakeholders have different objectives and information asymmetry. In cybersecurity compliance, system owners and providers generally have more information about control operations than customers, auditors, and regulators. Continuous compliance reduces this asymmetry through timely, attributable evidence.

4. Definitions and core constructs

Table 1 summarizes widely used definitions of constructions that overlap with, or enable, continuous

compliance. The table is intended to clarify terminology and provide citable anchors for future work.

Table 1. Definitions used in continuous compliance discourse

Construct	Source	Definition (verbatim or tightly paraphrased)	How it relates to continuous compliance
Continuous monitoring	NIST CSRC Glossary (CNSSI 4009 / SP 800-137)	Maintaining ongoing awareness to support organizational risk decisions.	A foundation for "continuous", but not sufficient without obligation mapping and assurance context.
Information security continuous monitoring (ISCM)	NIST SP 800-137	Maintaining ongoing awareness of information security, vulnerabilities, and threats to support risk management decisions.	Directly informs evidence and telemetry collection for controls.
Monitor step purpose (RMF)	NIST SP 800-37 Rev. 2 (Monitor step)	Maintain ongoing situational awareness about the security and privacy posture to support risk management decisions.	Links continuous activities to life-cycle risk governance.
Continuous monitoring program	NIST CSRC Glossary (SP 800-37 Rev. 2)	A program established to collect information using pre-established metrics, utilizing information available through implemented controls.	Operationalizes "continuous" through metrics and recurring evidence collection.
SOC 2 examination	AICPA SOC 2 overview	A report on controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy.	Represents an assurance regime that benefits from continuous evidence pipelines.
Continuous auditing (traditional definition)	CICA/AICPA (as cited by Vasarhelyi et al., 2012)	A methodology that enables independent auditors to provide written assurance using reports issued near the occurrence of events.	A sibling concept: continuous compliance supports continuous assurance by improving the timeliness of evidence.
Continuous controls monitoring (CCM)	Deloitte (Risk consulting)	A technology-based solution to continuously monitor processes and transition from sample-based testing to monitoring full populations.	Represents a control-testing approach that can be embedded in continuous compliance.
Continuous controls monitoring (CCM)	Bitsight glossary	Ongoing, automated collection and analysis of	Aligns to evidence/telemetry plus

		data about security and compliance controls to verify they operate effectively in near real time.	ongoing verification of controls.
Policy-as-code	Palo Alto Networks Cyberpedia	Policies are defined, updated, shared, and enforced using code.	Enables controls to be testable/enforceable continuously and supports consistency.
Compliance as code (contrast)	Trend Micro research notes	A broader perspective of continuously monitoring for compliance and enabling automated remediation steps when issues arise.	Captures a common engineering framing of continuous compliance and remediation workflows.

5. Core conceptual model

Continuous compliance is defined here as an instrument that enables organizations to maintain and demonstrate ongoing adherence to compliance obligations by continuously designing, verifying, and evidencing controls aligned with cyber risk governance objectives.

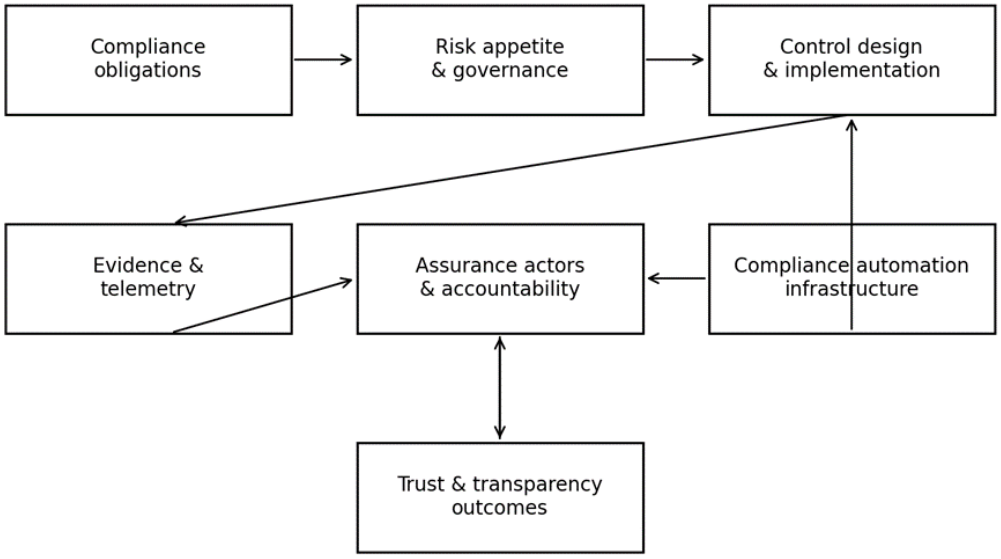


Figure 1. Core model: obligations → governance → controls → evidence → assurance → trust (enabled by automation)

5.1 Seven interacting aspects

- Compliance obligations: Requirements from laws/regulations, contracts, standards, customer requirements, and internal policies defining what must be true.
- Risk appetite and governance: Decision rights, oversight, escalation, and exception handling that prioritize obligations and define acceptable risk.
- Control design and implementation: Safeguards operationalizing obligations, including scope,

frequency, expected evidence, and failure modes.

- Evidence and telemetry: Observable data that demonstrates control operation (logs, configurations, CI/CD attestations, scans, tickets) with integrity and timeliness.
- Assurance actors and accountability: Control owners, GRC teams, auditors, customers, and regulators who define evidence sufficiency and accountability.
- Compliance automation infrastructure: Tooling and processes enabling continuous verification and evidence capture (policy-as-code, integrations, evidence repositories).
- Trust and transparency outcomes: Reduced information asymmetry, improved audit readiness, faster drift detection, clearer reporting, and stronger stakeholder confidence.

6. Field examples

The model can be instantiated across common assurance regimes. For SOC 2, continuous evidence pipelines reduce audit scrambling and support customer due diligence. For PCI DSS environments, continuous drift detection and recurring testing reduce the likelihood of control gaps. For ISO/IEC 27001 programs, continual improvement processes benefit from structured evidence repositories and recurring governance workflows.

7. Discussion and future research opportunities

7.1 Practical implications

Continuous compliance is not simply a tool purchase. Automation sits within a broader governance-to-evidence system that requires obligation clarity, control ownership, evidence sufficiency alignment, and exception handling. Monitoring without obligation mapping can create noise rather than trust.

7.2 Research agenda

Design science research (artifact-building):

- RQ1: What reference architectures best support obligation–control–evidence mapping across hybrid/cloud environments?
- RQ2: How should policy-as-code and control-as-code artifacts be designed to be both engineer-friendly and audit-valid?
- RQ3: What maturity models can measure continuous compliance capability beyond tool adoption (evidence integrity, control reliability, exception governance)?
- RQ4: Which evidence integrity mechanisms (e.g., signing, immutability, provenance) improve assurance outcomes relative to cost?
- Behavioral and empirical research:
- RQ5: How does continuous compliance change incentives, control ownership, and cross-team accountability?
- RQ6: Where do diminishing returns appear in compliance automation investments across control domains?
- RQ7: Does continuous compliance measurably improve security outcomes (incidents, response), or primarily assurance outcomes?
- RQ8: How do different stakeholders define sufficient evidence, and how do those differences influence system design and outcomes?

8. Limitations

This fundamentals paper prioritizes conceptual clarity and model utility over exhaustive empirical validation. Definitions and constructions are drawn from influential standards, assurance guidance, and widely used practitioner interpretations. Future work should test the model empirically across industries and assurance regimes.

9. Conclusion

Continuous compliance is increasingly adopted as organizations seek always-on assurance in fast-changing environments. This paper clarifies core constructs, provides a seven-aspect conceptual model, and outlines a research agenda to guide future IS research and practice.

Declaration of Conflicting Interests

The authors declare no potential conflicts of interest with respect to the research, authorship and publication of this article.

Funding

The author received no financial support for the research, authorship and publication of this article.

References

NIST CSRC Glossary: Continuous Monitoring. https://csrc.nist.gov/glossary/term/continuous_monitoring
NIST SP 800-137: Information Security Continuous Monitoring (ISCM). https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf
NIST SP 800-37 Rev. 2: Risk Management Framework (Monitor step). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
NIST CSRC Glossary: Continuous Monitoring Program. https://csrc.nist.gov/glossary/term/continuous_monitoring_program
AICPA: SOC 2 overview. https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2
Vasarhelyi, M. A., et al. (2012) – Continuous auditing definition (CICA/AICPA cited). https://www.sciencedirect.com/science/article/abs/pii/S1467089512000425
Deloitte: Continuous Controls Monitoring. https://www.deloitte.com/global/en/services/consulting risk/services/continuous-controls-monitoring.html
Bitsight Glossary: Continuous Controls Monitoring. https://www.bitsight.com/glossary/continuous-controls-monitoring
Palo Alto Networks Cyberpedia: Policy-as-code. https://www.paloaltonetworks.com/cyberpedia/what-is-policy-as-code
Trend Micro Research: Policy-as-code vs Compliance-as-code. https://www.trendmicro.com/en_us/research/23/c/policy-as-code-vs-compliance-as-code.html
ISO 37301: Compliance management systems. https://www.iso.org/standard/75080.html