EVALUATION SUBJECT

Sample Tool v1.0

Sample Company · 2026Q2 · Regulatory & Compliance Alignment

The following represents Levix Labs' assessment of the tool's alignment with major regulatory and compliance frameworks as observed during the 2026Q2 evaluation. This is not a certification or legal compliance determination — it reflects evaluator observations based on documentation review and testing. Organizations with specific compliance obligations should conduct independent verification.

1	4	1	0
ALIGNED	PARTIAL	GAP IDENTIFIED	NOT APPLICABLE

FRAMEWORK STATUS

FRAMEWORK	STATUS	SUMMARY
SOC 2 Type II	PARTIAL	The organization maintains documented security policies and access controls, but has not completed a formal SOC 2 Type II audit as of this evaluation period. Evidence of controls is present; independent attestation is outstanding.
GDPR	PARTIAL	Data handling practices include basic retention policies and documented data flows. A formal Data Protection Impact Assessment (DPIA) was not provided for review and should be completed before processing EU personal data at scale.
HIPAA	GAP IDENTIFIED	Current access control architecture does not support the audit logging granularity required for HIPAA compliance. A Business Associate Agreement (BAA) framework is not yet in place. Significant remediation is required before use in covered healthcare contexts.

EU AI Act	PARTIAL	The tool operates in a domain that may qualify as high-risk under the EU AI Act depending on deployment context. Risk management documentation is present but does not fully address the Act's transparency and human oversight requirements.
NIST AI RMF	PARTIAL	The organization demonstrates awareness of AI risk management concepts and maintains internal documentation aligned to the GOVERN and MAP functions. MEASURE and MANAGE functions are partially implemented; formal adoption of the full RMF has not been completed.
CCPA	ALIGNED	Documented data subject rights procedures are in place and the organization maintains a privacy policy consistent with CCPA requirements for the current scope of data processing.

Context & Guidance for Regulated Deployments

The tool's Safety dimension received a grade of BB in this evaluation period. The following guidance addresses the most relevant compliance gaps observed and their practical implications for organizations operating in regulated industries.

For Healthcare Organizations (HIPAA)

HIPAA-covered entities and business associates should not deploy this tool in clinical or administrative workflows involving protected health information (PHI) without first completing the access control and audit logging improvements identified in the full report. A signed BAA must be in place before any PHI is processed. The current architecture is not structurally incompatible with HIPAA, but requires targeted remediation before compliant use is possible.

For Financial Services Organizations

Organizations subject to SOC 2, SEC, or FINRA requirements should confirm that the tool's data handling practices meet their specific contractual and regulatory obligations. The absence of a completed SOC 2 Type II report is a typical barrier in financial services vendor review processes. Request updated attestation status from the vendor before signing data processing agreements.

For Organizations Subject to the EU AI Act

Organizations deploying this tool within the EU should perform an independent high-risk classification assessment based on their specific deployment context. If the tool is used in consequential decision-making, documentation of human oversight mechanisms and transparency measures will be required. The vendor's current documentation partially supports this but should be supplemented with deployment-specific assessments.

For Non-Regulated Organizations

Organizations without specific regulatory compliance requirements are well-positioned to deploy this tool in its current state. The Levix Procurement Brief provides a concise deployment recommendation and conditions summary for this context. Basic data governance practices — defined retention, access logging, and clear data processing agreements — are recommended regardless of regulatory obligation.

IMPORTANT NOTICE

These regulatory alignment notes are informational and do not constitute legal advice, a compliance certification, or a legal determination of any kind. Organizations should consult qualified legal and compliance counsel before making regulatory compliance decisions. Levix Labs' assessment reflects evaluator observations during the 2026Q2 rating period and may not reflect changes made after the evaluation window closed.