

Compliance for vibe-coded apps

<https://prompt-to-prototype.com/governance/compliance/> · as of 2026-10-22

Most compliance duties attach to what an app does and the data it touches, not to whether AI helped build it. For a North American business, privacy, sector and consumer-protection laws usually apply first; [SOC 2](#) and ISO audits ask whether your controls cover these apps; the [EU AI Act](#) matters only when an AI feature reaches the EU. Auditors want evidence that you know which apps exist, who owns them, and that controls scale with risk. As of October 2026.

Who this is for

Compliance, risk and audit leads, and IT managers who answer customer questionnaires about vibe-coded or citizen-developed apps. About 14 minutes.

Not legal advice

Not legal advice. This page summarizes laws as of October 2026 for a general audience. It was written with an AI legal-research persona and hasn't been reviewed by a lawyer for your situation. Ask your counsel.

What applies when?

Every worker-built app sits in one of four risk tiers (Sandbox, Team, Important or Critical), set by the highest answer to six questions about its data, users, internet reach, dependence, decisions about people and actions, and two floors apply at every tier. The [six tier questions](#) are also your legal screen: each situation below starts from an intake answer. The detail of each law, with its thresholds and dates, lives on [US and Canadian laws for AI-built apps](#); this table tells you which obligation to look up and which control you already have.

Fast-moving

As of October 2026. Check the review date.

Situation	What applies (type)	Who it applies to	Control on this site that helps	Detail
Holds personal data about customers or staff (Q1(b), Q1(c))	State privacy laws, PIPEDA, Quebec Law 25 (legal requirement)	Businesses over each law's thresholds; Law 25 for anyone handling Quebec residents' information	Data classes, data-owner sign-off, the jurisdiction flag	State laws , Canadian laws , data handling

Situation	What applies (type)	Who it applies to	Control on this site that helps	Detail
Health, financial or card data (Q1(c), or Q1(d) for card data and covered-entity PHI; C1)	HIPAA; GLBA Safeguards Rule (legal requirement); PCI DSS 4.0.1 (contractual, through card brands and acquirers)	HIPAA covered entities and business associates; non-bank financial institutions; anyone storing, processing or transmitting card data	Confidential and Restricted data classes, standard downgrade 2, approved tools per data class	Federal laws, C1 below
Helps decide about people (Q5)	FCRA and ECOA, CCPA automated-decision rules and Colorado SB 26-189 (both from 1 Jan 2027), NYC Local Law 144, Quebec s. 12.1 (legal requirement)	Employers, lenders, insurers, landlords and others making the covered decisions	Meaningful human review, Q5 answers, graduation	Apps that make decisions about people
Customer-facing AI feature or claims about AI (Q2(c), M2)	FTC Act §5 and state consumer-protection laws (legal requirement); state chatbot-disclosure laws	Most for-profit businesses	The claims register ; the AI-disclosure check at Important	Chatbot disclosure laws
Output feeds the ledger or a tested control without recomputation (Q4(d1))	SOX §404 and ICFR (legal requirement for SEC registrants; an auditor or lender expectation for private companies)	SEC registrants; private companies whose auditors or lenders ask	Q4(d1) sets Critical; the audit-scope flag is yes, so the compliance owner sets change and evidence requirements	Federal laws
Inside a SOC 2, ISO/IEC 27001, PCI DSS or SOX scope (audit-scope flag)	SOC 2 and ISO certification scope and PCI DSS (contractual; no statute requires them); SOX (legal requirement for SEC registrants)	Businesses that issue a SOC 2 report, hold a certificate, are in PCI scope or report under SOX	The audit-scope flag , routed to the compliance owner	SOC 2 below
A customer questionnaire or contract asks about AI (C4)	The contract you signed; FTC Act §5 if you misstate your controls	Anyone answering	The evidence pack (C4 below)	Contract terms
An internet-reachable app leaks data (Q3(b))	State breach laws, HIPAA, GLBA, SEC Form 8-K Item 1.05, PIPEDA (legal requirement)	Varies by law	Floor 2, the exposure scan, incident routing from the registry	Breach and incident duties
EU people, staff or AI output used in the EU (jurisdiction flag)	GDPR (Art. 3); the EU AI Act for AI features (legal requirement where they reach you)	Businesses with an EU establishment, EU customers, or AI output used in the EU	The jurisdiction flag routes to counsel	The EU AI Act page

The labels matter. A **legal requirement** comes from a statute or regulation. A **regulator expectation** is guidance that signals how a regulator will judge you. **Good practice** is what this site recommends. SOC 2, ISO certification and PCI DSS are none of these on their own: they bind you because a contract or a card agreement says so.

Don't: start from EU law

For a US or Canadian business, privacy, sector and consumer-protection law applies first, and the EU AI Act touches only AI features whose output reaches the EU. The Act regulates AI systems by their use. Code an AI helped write isn't an AI system, so there's no AI Act duty to log "AI involvement in code".¹ Keep change history for engineering and audit reasons, and say so.

What evidence will an auditor ask for?

Auditors' questions are predictable: which apps exist, who owns them, who can change them, how changes were tested and approved, who has access, and what happened when someone left. The answers should come out of records the program already keeps, not out of a scramble when the request arrives. The table follows the [gate matrix](#); it adds nothing the gates don't already require, except where marked good practice.

Evidence	Comes from	Sandbox	Team	Important	Critical
Registry export: every app, owner, tier, data class, status	App registry	sandbox workspace list	app record	app record, plus data-owner sign-off for Confidential or Restricted data	+ graduation plan
Intake record: six answers, flags, decision	Intake	—	yes	yes	yes
Test evidence	The builder's tests	—	own test cases pass before every release	+ negative access tests	+ independent tests
Review evidence	Verify	self-check (recommended)	recorded self-check	+ business review and technical check records	+ security review
Access evidence	Sign-in and access reviews	private workspace	SSO	SSO, deny-by-default data rules	+ quarterly access review
Change history	Version control or the platform's audit log	—	version history you can roll back, with each release's tests and self-check (gate)	same, plus each release's business review and technical check records (gate); a named approver per release is good practice	same, through IT's change process
Exposure scan results	The scheduled external scan	—	good practice	monthly	monthly
Scheduled review records	Registry	at 90 days	every 12 months	every 6 months	every 6 months
Owner-leaves handling	When the builder leaves	quarantine	handover record	handover record	handover record
Retirement record	Retire	deletion note	checklist	checklist, with data disposal	checklist, with data disposal

Audit-scope apps, at any tier. If the audit-scope flag is yes, the compliance owner sets the change-management and evidence requirements, whatever the tier, and go-live waits until they've been set. There's no tier floor: an access-review tracker can stay at Team and still need retained change history for the whole audit period. The `audit_scope`, `controls_evidenced` and `change_history_location` fields on the [app record's audit sheet](#) hold the answers.

Completeness is the first thing an auditor tests, and self-reported inventories undercount (A-005). Keep the discovery evidence from [finding the apps you already have](#) next to the registry export, so you can show how you know the list is whole.

How do worker-built apps fall into SOC 2 scope?

SOC 2 is a CPA attestation against the AICPA's Trust Services Criteria.² No statute requires it. The obligation comes from customer contracts, security addenda and questionnaires, and a misstated scope can become a contract dispute or, if you tell customers something untrue, an FTC Act deception issue. A business that only *receives* vendors' SOC 2 reports is a user entity: its job is to run the complementary user entity controls (CUECs) those reports list. You don't need a "SOC 2 for AI", because the criteria you already report against cover these apps.

A worker-built app enters the system boundary through what it touches or does, not how it was built. In counsel's reading of the AICPA definitions (an inference, not AICPA text), it's inside the boundary if any of these is true:

- 1. **It helps deliver the in-scope service:** it processes, stores or moves customer data for that service (a ticket-triage tool, a customer-data export, a report customers receive).
- 2. **It performs or evidences a control the report describes:** an access-review tracker, a change-approval log, an incident register, vendor-review records, an onboarding or offboarding checklist. Its output is audit evidence, so the auditor will test that it's complete and accurate.
- 3. **It holds privileged access** to in-scope systems: an agent or automation with a token to the production database, the CRM, the identity provider or the cloud console.
- 4. **It holds data designated confidential** under the report's commitments, even outside the production stack.

An app that touches none of these is outside the boundary. That doesn't make it unregulated: privacy, employment and accessibility law still apply.

Criterion	Why worker-built apps hit it	Evidence the auditor will ask for
CC6.1 (logical access; the inventory point of focus)	Every app is an information asset and a point of access; the 2022 points of focus extend access controls to "IT tools" and to system and service accounts ³	Registry export; SSO enforcement; the list of service identities and OAuth grants
CC6.2, CC6.3 (provisioning, removal, least privilege)	App-managed user lists that bypass SSO; builders who are also approvers	Joiner and leaver evidence that covers the app; separation of builder and approver at Important and Critical

Criterion	Why worker-built apps hit it	Evidence the auditor will ask for
CC6.6, CC6.7 (outside threats, data movement)	Public links; data sent to AI model services	The hosting pattern; AI destinations limited to approved tools
CC7.2–CC7.4 (monitoring, incidents)	An app with no logs or owner can't be monitored	Logging (good practice from Team; checked at the technical check from Important); incident routing from the registry
CC8.1 (change management)	AI-assisted builders change apps fast, often live; prompt and agent-configuration changes are software changes	Change history, test evidence, approval records by tier
CC9.2 (vendors)	AI app builders, model services and hosts are vendors, and may be subservice organizations	The approved-tools list with vendor review, each vendor's SOC report and its CUECs
C1.1, C1.2 (confidential data, disposal)	Copies of confidential data in builder tools, prompts and exports; retirement without deletion	Data class and retention on the app record; a deletion step at retirement
CC3.2, CC3.4 (risk assessment, change in the environment)	A wave of AI-built apps is a change in the technology environment	A risk assessment that names worker-built apps, with the tier model as the method

Points of focus aren't requirements: the criteria document says using them "does not require an assessment of whether each point of focus is addressed".² Processing Integrity, Availability and Privacy apply only if your report includes them.

The system description. If worker-built apps sit inside the boundary, the description must account for them. An AI building or hosting platform that runs an in-scope app may be a subservice organization (carved out or inclusive), and moving an in-scope process onto worker-built apps can be a significant change to disclose (secondary sources; the AICPA description criteria are gated).³ A vendor CUEC such as "the customer protects its API keys" is then performed, or not, inside the app that holds the token.

What auditors typically ask. We found no AICPA guidance written for AI-built apps. One Big Four practice notes that such apps "often [sit] outside the IT Control environment, which significantly expands the scope of audits".⁴ Expect questions on inventory completeness, who can change the app and how changes are approved, access and service-account scope, the reliability of any report the app produces as evidence, which platform hosts it, and what happens when the builder leaves. Apps with no history can't be sampled across the audit period, which tends to produce an exception.

Illustrative composite

A team builds a faster tracker for quarterly access reviews, and the builder edits it live with no version history. At the next Type 2 audit the auditor can't confirm the tracker's logic was the same all year, so the access-review control gets an exception. Answering yes to the audit-scope flag at intake would have sent it to the compliance owner, who would have asked for retained change history before go-live.

ISO/IEC 27001 and 42001. If you're certified to ISO/IEC 27001:2022, the question is whether worker-built apps fall inside the scope statement. If they do, Annex A controls such as 5.9 (inventory), 8.25 (secure development) and 8.32 (change management) apply to them.⁵ ISO/IEC 42001:2023 matters only if you run an AI management system; its scope then covers AI features your staff build.⁶ Neither certificate comes from following this site. The control-by-control map is on the [standards crosswalk](#).

Depends on your circumstances

Depends on your circumstances (C1): regulated data

If you hold health, financial or card data, put it only in builder tools approved for its class. Financial data such as bank account numbers is Confidential (Q1(c)). Full card numbers, and health information held by a HIPAA covered entity or business associate, are Restricted (Q1(d)) and stay out of builder tools unless IT approves the tool and pattern. A HIPAA covered entity or business associate needs a business associate agreement with any vendor that handles PHI for it, and the app belongs in its risk analysis. Under PCI DSS 4.0.1, sending card data to a tool brings that tool into scope, which you must document and confirm (Req. 12.5.2), and makes its vendor a service provider you must manage (Req. 12.8). Log retention and data-retention detail is on [data handling](#).⁷ Banks: model-risk guidance is SR 26-2 (April 2026), which superseded SR 11-7.⁸ Broker-dealers: FINRA Regulatory Notice 24-09 says existing supervision and communications rules apply to generative AI.⁹

Depends on your circumstances (C2): public bodies

US federal agencies follow OMB M-25-21, which replaced M-24-10: an AI use-case inventory, an AI strategy and minimum practices for high-impact AI.¹⁰ Prompts, outputs and app records may be public records or agency records subject to access-to-information requests; ask your records officer. Canadian federal institutions follow the Directive on Automated Decision-Making for systems that make or support administrative decisions ([decisions about people](#)).

Depends on your circumstances (C3): cross-border data

When an AI service or host processes data in another country, check three things: Quebec Law 25 s. 17 (an assessment and written agreement before information leaves Quebec), the DOJ bulk sensitive-data rule (vendors linked to countries of concern), and, for EU data, the [EU-US transfer route](#). The [contract terms](#) for data location are where you record the answer.

Depends on your circumstances (C4): customers ask about your AI use

Build one evidence pack and answer every questionnaire from it: a registry summary (counts by tier, owners named), the acceptable-use policy, the approved-tools list by data class, the tier model, a sample of review and access evidence, and your incident process. Don't promise what you can't show. If a questionnaire asks whether a control covers "all applications", check that the registry backs that up before you tick yes, and check what your customer contracts already promise about AI use.

When should you stop and escalate?

These events pause the app (freeze changes; keep it running only if stopping it causes more harm) and go to the compliance owner and counsel the same day:

- Restricted data turns up in a tool that isn't approved for it.
- An internet-reachable app exposed personal data. Breach clocks may be running ([breach and incident duties](#)). Preserve the logs, because whether a notice is owed often turns on whether anyone accessed the data.
- An audit-scope app was changed with no retained history, or its owner left without a handover.
- An approved vendor changes its sub-processors, data location or training terms.
- Output is found feeding the ledger or a tested control without recomputation (Q4(d1)), or a feature starts scoring, ranking or flagging people (Q5). Both mean re-tiering.

Write down the go or no-go decision before the app resumes. If litigation or an investigation is likely, the hold has to reach the app's data, its prompts and its AI logs ([incident response](#)).

Keep a claims register

Every public or customer-facing statement about your AI use, or about an AI feature, goes in a register with the evidence behind it. Regulators have acted against unsupported AI claims: in March 2024 the SEC settled with two investment advisers over false statements about their AI use,¹¹ and the FTC's September 2024 "Operation AI Comply" targeted deceptive AI claims.¹² The register has five columns: the claim, where it appears, the evidence, the owner, and the date last checked. Recheck it at each scheduled review and whenever a feature or model changes.

Don't: tell anyone you're compliant because you follow this framework (AP16)

This framework doesn't make anyone compliant with a law or certified to a standard. Say "we map our controls to the NIST AI RMF and SOC 2", keep the mapping on the [standards crosswalk](#), and keep the evidence. See [AP16: AI-washing claims](#).¹¹

Don't: cite superseded guidance

OMB M-24-10 was rescinded by M-25-21 (April 2025),^{[10](#)} and SR 11-7 was superseded by SR 26-2 (April 2026).^{[8](#)} Policies, questionnaires and audit responses that still cite them look stale to an auditor and may point staff at the wrong rules.

Questions to ask your counsel

1. Are worker-built apps inside the scope of our SOC 2 or ISO audit, and does our system description need updating?
2. Does any AI app-building or hosting platform we use count as a subservice organization for our report, and do we present it carved out or inclusive?
3. Which complementary user entity controls in our vendors' SOC reports are now performed inside worker-built apps?
4. Which of our customer contracts, security addenda or questionnaire answers make promises about AI use or about controls covering "all applications"?
5. Which worker-built apps support SOX key controls or financial reporting, and what evidence will our auditors expect?
6. Are we a HIPAA covered entity or business associate, a GLBA financial institution, or in PCI scope, and which AI vendors need a BAA, service-provider terms or a PCI responsibility matrix?
7. Which of our public or customer-facing claims about AI features need substantiation under the FTC Act and state consumer-protection laws?
8. Are prompts, outputs and agent logs covered by our retention schedule and litigation-hold process, and can our AI tools suspend deletion on a hold?
9. Do EU or UK laws reach us, and could a worker-built AI feature make us a provider under the EU AI Act?

Assumptions and evidence

- **A-019** (Medium): We expect regulators and auditors to favor enabled, inventoried, risk-tiered use over bans. That's well supported for the public sector and a hypothesis by analogy for private businesses; test it by checking each new enforcement action and audit-guidance release at the quarterly review.
- **A-005** (Medium): We expect self-reported inventories to undercount; test it by comparing registry counts with discovery-scan counts before the first audit that relies on the registry.
- Evidence: the AICPA criteria (read from a third-party copy of the 2020 edition, with 2022 changes from a Big Four summary), statutes, regulator pages and one auditor-side article. We found no audit-standard guidance written for AI-built apps, and no controlled study of audit outcomes for worker-built apps.
- Facts on this page are as of October 2026.

Related

- [US and Canadian laws for AI-built apps](#): each law's scope, thresholds and dates.
- [Apps that make decisions about people](#): the Q5 trigger in depth.

- [The EU AI Act and worker-built apps](#): when EU AI law reaches a North American business.
- [Standards crosswalk for worker-built apps](#): which framework controls the gates support.
- [App registry](#): the inventory every audit starts from.
- [IP and licensing for AI-built apps](#): ownership, open-source licenses and provenance records.

-
1. Regulation (EU) 2024/1689 (AI Act), Art. 3(1) definition of "AI system", <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> [statute; EUR-Lex returned a challenge page to our tools, so the text was checked on secondary article explorers], accessed 2026-10-22.
 2. AICPA, *2017 Trust Services Criteria (With Revised Points of Focus, 2022)*, TSP §100, <https://www.aicpa-cima.com/resources/download/2017-trust-services-criteria-with-revised-points-of-focus-2022> [standard; free registration required]. Criterion wording and the points-of-focus quote (§1.04) were read from the March 2020 edition as reproduced by a vendor, <https://arpio.io/wp-content/uploads/2020/08/trust-services-criteria.pdf> [vendor-hosted copy], accessed 2026-10-21.
 3. EY, *To the Point* 2022-13, "AICPA revises guidance on applying its Trust Services Criteria and SOC 2 Description Criteria", 2 Nov 2022, <https://ey.com/content/dam/ey-unified-site/ey-com/en-us/technical/accountinglink/documents/ey-ttp17549-221us-11-02-2022.pdf> [secondary; source for the 2022 points of focus and the description-criteria points], accessed 2026-10-21.
 4. Deloitte UK, "Feeling the Vibe: Navigating the new generation of low-code tools", 24 Oct 2025, <https://www.deloitte.com/uk/en/Industries/financial-services/perspectives/navigating-the-new-generation-of-low-code-tool.html> [secondary; auditor-side view], accessed 2026-10-22.
 5. ISO, ISO/IEC 27001:2022, Information security management systems, <https://www.iso.org/standard/27001> [standard; paid text, control numbers from the 2022 Annex A], accessed 2026-10-22.
 6. ISO, ISO/IEC 42001:2023, AI management systems, <https://www.iso.org/standard/81230.html> [standard], accessed 2026-10-21.
 7. PCI Security Standards Council, PCI DSS v4.0.1 (11 Jun 2024), Requirements 12.5.2 and 12.8, https://www.pcisecuritystandards.org/document_library/ [standard; the library needs a click-through, so requirement text was confirmed against reproductions], accessed 2026-10-22.
 8. Board of Governors of the Federal Reserve System, SR 26-2, Revised Guidance on Model Risk Management, 17 Apr 2026, <https://www.federalreserve.gov/supervisionreg/srletters/SR2602.htm> [regulator], accessed 2026-10-22.
 9. FINRA, Regulatory Notice 24-09, 27 Jun 2024, <https://www.finra.org/rules-guidance/notices/24-09> [regulator], accessed 2026-10-21.
 10. OMB, Memorandum M-25-21, 3 Apr 2025, <https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-21-Accelerating-Federal-Use-of-AI-through-Innovation-Governance-and-Public-Trust.pdf> [primary], accessed 2026-10-21.
 11. SEC, "SEC Charges Two Investment Advisers with Making False and Misleading Statements About Their Use of Artificial Intelligence", press release 2024-36, 18 Mar 2024, <https://www.sec.gov/newsroom/press-releases/2024-36> [regulator], accessed 2026-10-21.
 12. FTC, "FTC Announces Crackdown on Deceptive AI Claims and Schemes", 25 Sep 2024, <https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes> [regulator], accessed 2026-10-21.

Prompt to Prototype, Compliance for vibe-coded apps, <https://prompt-to-prototype.com/governance/compliance/>, as of 2026-10-22. Licensed [CC BY-SA 4.0](#).