

Standards crosswalk for worker-built apps

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

Use ISO/IEC 42001 or the NIST AI RMF for AI governance, and the security frameworks you already run for the controls. In practice that means NIST CSF 2.0, SOC 2, ISO/IEC 27001 and PCI DSS 4.0.1 for controls, plus build-security standards for the apps themselves: SSDF, SLSA, the OWASP Citizen Development, LLM and Agentic Top 10s, MCP security practices, and WCAG 2.2 for accessibility. None of them can be "complied with" by reading this site. The crosswalk maps each one to a lifecycle stage and the page that implements it, as of October 2026.

Who this is for

Security and compliance leads, auditors, and platform engineers who need to show which existing controls cover worker-built apps. About 12 minutes.

Not legal advice

Not legal advice. This page summarizes standards and frameworks as of October 2026 for a general audience; frameworks aren't law, and the laws that apply are on [US and Canadian laws for AI-built apps](#). It was written with an AI legal-research persona and hasn't been reviewed by a lawyer for your situation. Ask your counsel.

How do these standards fit together?

They answer different questions, so you need a few of them, not one.

- The governance shell: the NIST AI RMF or ISO/IEC 42001 gives you policy, roles, risk tolerance and impact assessment. Both describe outcomes and management processes; neither is a control checklist.
- The controls you already run: NIST CSF 2.0, ISO/IEC 27001, SOC 2 and PCI DSS already cover inventory, access, change, vendors and incidents. Worker-built apps belong inside those controls, not in a parallel set.
- The secure build: the SSDF and SLSA set the practices and supply-chain levels for any app, AI-built or not. The OpenSSF guide covers how builders instruct coding assistants. The OWASP Citizen Development Top 10 is the risk list for worker-built apps.
- AI features and agents only: the OWASP LLM and Agentic Top 10s and the MCP security practices apply when an app **contains** an AI feature or agent, or when builders run agentic tools with real permissions.
- Accessibility: WCAG 2.2 AA is the test for apps people outside the business use, and good practice for internal apps staff must use.

Building an app with AI help doesn't change which of these apply. What the app does, and what it holds, does. That's the same principle the [six tier questions](#) use: 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 crosswalk

Fast-moving

As of October 2026. Check the review date.

Standard	Version and date	Status	What it asks	Lifecycle stage	Where this site covers it
NIST AI RMF (AI 100-1) ¹	1.0, Jan 2023	Voluntary; under revision	Four functions (Govern, Map, Measure, Manage); documented risk tolerance, context mapping, measurement, risk treatment	Program-wide; intake (Map); verify (Measure); operate (Manage)	Governance, risk tiers, evaluate an AI feature
NIST AI 600-1, Generative AI Profile ²	Final, Jul 2024	Voluntary	Twelve generative AI risks (confabulation, information security, data privacy, IP and others) with suggested actions mapped to the RMF	Intake, verify, operate	Secure AI features
NIST CSF 2.0 ³	2.0, Feb 2024	Voluntary	Six functions (Govern, Identify, Protect, Detect, Respond, Recover), including asset inventory and supply-chain risk	All stages	Reuse table below
NIST Cyber AI Profile (IR 8596) ⁴	Preliminary draft, Dec 2025	Draft; not final	A CSF 2.0 profile for securing AI systems and defending against AI-enabled attacks	Build, deploy, operate	Watch item
NIST SSDF (SP 800-218) ⁵	v1.1, Feb 2022; Rev. 1 draft, Dec 2025	v1.1 final; Rev. 1 still a draft	Secure-development practice groups: prepare the organization (PO), protect the software (PS), produce well-secured software (PW), respond to vulnerabilities (RV)	Build, verify, deploy, change	Security checklist, change
NIST SP 800-218A ⁶	Final, Jul 2024	Voluntary	SSDF profile for producers of generative AI and foundation models : model and data provenance, training-data integrity, weight protection	Build (only if you train or fine-tune models)	Not used for AI-assisted building
ISO/IEC 42001 ⁷	2023, first edition	Certifiable	An AI management system: AI policy, risk and impact assessment, Annex A lifecycle controls	Program-wide; intake (impact assessment)	Governance, intake

Standard	Version and date	Status	What it asks	Lifecycle stage	Where this site covers it
ISO/IEC 27001 ⁸	2022	Certifiable	An information security management system with Annex A controls (inventory, access, supplier, secure development, change, logging)	All stages	Reuse table below, compliance
SOC 2 Trust Services Criteria ⁹	2017 criteria, 2022 points of focus	Attestation by a CPA; contractual	Security (common criteria CC1–CC9), plus Availability, Processing Integrity, Confidentiality and Privacy where in scope	All stages	SOC 2 scoping
PCI DSS ¹⁰	v4.0.1, Jun 2024	Contractual (card brands and acquirers); v4.0 retired end of 2024	Twelve requirement families for anyone storing, processing or transmitting card data, including scope (Req. 12.5.2) and service providers (Req. 12.8)	Intake (data class), build, operate	Data handling, compliance C1
OWASP Citizen Development Top 10 ¹¹	No version stated; content path dated 2022	Community risk list	Ten risks for low-code, no-code, AI-assisted and agent-built apps, CD-SEC-01 Blind Trust to CD-SEC-10 Security Logging and Monitoring Failures	Intake, build, verify, retire	Security checklist mapping
OWASP Top 10 for LLM Applications ¹²	2025 edition	Community risk list	LLM01 Prompt Injection to LLM10 Unbounded Consumption	Intake (threat model), build, verify	Secure AI features
OWASP Top 10 for Agentic Applications ¹³	2026 edition, released Dec 2025	Community risk list	Agent risks such as goal hijack, tool misuse, identity and privilege abuse, and rogue agents	Build, deploy, operate	MCP and agents, coding agents
MCP specification and security best practices ¹⁴	2026-07-28	Protocol specification	Explicit user consent before tool calls; tool descriptions treated as untrusted; no token passthrough; least-privilege scopes	Build, deploy, operate	MCP security baseline
SLSA ¹⁵	v1.2	Approved specification	Supply-chain levels for build provenance, and a new Source track for source history and review	Build, deploy, change	Security checklist
OpenSSF guide for AI code assistant instructions ¹⁶	1 Aug 2025	Community guidance	Put security requirements in the assistant's standing instructions; vet dependencies; run scanners on the output	Build, verify	Coding agents

Standard	Version and date	Status	What it asks	Lifecycle stage	Where this site covers it
WCAG 2.2 ¹⁷	W3C Recommendation, Oct 2023, updated Dec 2024	Referenced by law in some places (often at 2.1 AA)	Level A and AA success criteria, including six new A and AA criteria in 2.2 (four at AA: focus not obscured, dragging, target size, accessible authentication; two at A: consistent help, redundant entry)	Build, verify	Production readiness: accessibility

[Download the crosswalk as CSV](#) (updated 2026-10-22), with the same columns plus each page's full URL. *Prompt to Prototype, Standards crosswalk for worker-built apps*, <https://prompt-to-prototype.com/governance/standards/#crosswalk>, as of 2026-10-22. Licensed CC BY-SA 4.0. CC BY-SA 4.0's conditions apply when you share the material, which the license defines as providing it to the public. Using or adapting it inside your business usually isn't sharing; if you give your version to anyone outside the business, keep this credit line and license your changes under CC BY-SA 4.0. If the file and this page differ, the page wins.

Other government and industry texts are useful references but aren't part of the core stack: CISA's Secure by Design principles, aimed at software manufacturers and read here as "secure by default paved road",¹⁸ and Singapore IMDA's Model AI Governance Framework for Agentic AI (v1.5, May 2026), a practical government text on bounding agents.¹⁹

Don't: use the 2023 OWASP LLM list

The 2023 list (insecure output handling, training-data poisoning, model denial of service, insecure plugin design, overreliance, model theft) was replaced by the 2025 edition, which adds system prompt leakage, vector and embedding weaknesses, misinformation and unbounded consumption.¹² Checklists built on the old list miss current risks.

Don't: cite SP 800-218A for using AI to write code

SP 800-218A is for organizations that produce generative AI models and systems: training data, model weights, provenance.⁶ It gives no guidance on staff using AI to write code. For that, use the SSDF itself and the OpenSSF guide.

Reuse what you already have

Most of what this framework asks for is a control you already report on, applied to apps that were outside its reach. The table shows which framework clauses each gate or record supports, so you can extend existing evidence instead of writing new policies. "Supports" means the gate produces evidence for that control. It doesn't mean the control is met; your auditor or assessor judges that.

This framework's gate or record	NIST CSF 2.0	ISO/IEC 27001:2022 Annex A	SOC 2	ISO/IEC 42001 / AI RMF	Build standards and PCI DSS
App registry and discovery	ID.AM-02 (software and services), ID.AM-07 (data)	5.9 (inventory)	CC6.1 (inventory point of focus)	AI RMF GOVERN 1.6 (AI system inventory; AI features only)	CD-SEC-09 (asset management)
Intake and the six tier questions	ID.RA, GV.OC-03	5.12 (classification)	CC3.2, CC3.4	42001 A.5 (impact assessment) and AI RMF MAP 1.1, partial: AI features only	n/a
Approved tools and contract terms	GV.SC-05	5.19–5.23 (suppliers)	CC9.2	42001 A.10.3 (AI suppliers; if you run an AI management system)	PCI DSS Req. 12.8
SSO, deny-by-default data rules, access reviews	PR.AA-05	5.15, 5.18 (access)	CC6.1–CC6.3	n/a	PCI DSS Req. 7, 8
Tests, verify , technical check	PR.PS-06	8.25, 8.29 (secure development, testing)	CC8.1	42001 A.6.2.4 and AI RMF MEASURE 2.5, partial: AI features only	SSDF PW.7, PW.8
Change history and change review	ID.RA-07 (changes managed and recorded), PR.PS-01 (configuration management)	8.32 (change management)	CC8.1	n/a	SSDF PS.1; SLSA Source track
Dependency and license checks	GV.SC	5.32 (IP rights), 8.28 (secure coding, external libraries)	CC8.1	n/a	SSDF PW.4.1, PW.4.4, PS.3.2
Exposure scan and logging	DE.CM	8.15, 8.16 (logging, monitoring)	CC7.1, CC7.2	n/a	PCI DSS Req. 10, 11
Incident routing from the registry	RS.MA, RS.CO-02/03	5.24–5.28	CC7.3–CC7.5	n/a	PCI DSS Req. 12.10
Owner-leaves check	PR.AA	5.18 (access rights), 6.5 (responsibilities after termination or change)	CC6.2	n/a	n/a
Retirement with data disposal	ID.AM-08	8.10 (information deletion)	C1.2	n/a	PCI DSS Req. 3.2.1
AI feature evals and human review	n/a	n/a	PI1.x where in scope	42001 A.6.2.4, A.9.2–A.9.4 (responsible and intended use); AI RMF MEASURE 2.9, 2.11	OWASP LLM Top 10

"Partial" and "AI features only" mean the clause covers part of the gate, or applies only where the app has an AI feature or you run an AI management system; for other apps, don't count it. The control IDs come from each framework's published text or, for paid standards, their published control lists; check them against the edition your auditor uses. Where a gate maps to a law rather than a framework, the [compliance page's "what applies when" table](#) and [US and Canadian laws](#) carry it.

Depends on your circumstances (C4): customers rely on your certificate or report

If customers or contracts already rely on your ISO/IEC 27001 certificate or SOC 2 report, start from its scope statement, not from this table. Decide which worker-built apps are inside it (the [audit-scope flag](#) finds them), then extend the existing controls and evidence to those apps. Adding ISO/IEC 42001 makes sense when you build or run AI features at a scale that a customer or regulator asks you to manage formally.

Most likely failure. A team maps every gate to every framework and produces a crosswalk nobody uses. Keep it to the frameworks you're actually assessed against, plus the AI RMF or 42001 if you've adopted one. The cheaper alternative we rejected was a single new "AI controls" list: it duplicates controls you already test and gives auditors a second set of evidence to reconcile.

How do you say "aligned with" honestly?

Use words that match what you can show.

- **"We map our controls to the NIST AI RMF."** True if you keep the mapping and the evidence. The RMF is voluntary and outcome-based, so you can't be "compliant" with it.
- **"Our program is aligned with ISO/IEC 42001."** Acceptable only with a gap assessment behind it. Conformity to 42001 or 27001 means certification by an accredited body; mapping to it isn't certification.
- **"Our SOC 2 report covers worker-built apps in scope."** True only if the system description and testing include them.
- **"We use the OWASP Top 10 lists in threat modelling and review."** The OWASP lists are risk lists, not standards, so "OWASP compliant" means nothing.

Put each of these statements in the [claims register](#) with its evidence.

Don't: claim a framework because you follow this site (AP16)

Following this framework doesn't make a business compliant with, or certified to, anything. Unsupported claims about AI governance carry their own risk; regulators have acted against unsupported AI claims.^{[20](#)}

Superseded references to replace

If your policies or questionnaire answers cite any of these, update them:

Old reference	Current reference (as of October 2026)
OMB M-24-10 (US federal AI use)	OMB M-25-21 (April 2025) ²¹
SR 11-7 (bank model risk)	SR 26-2 (April 2026) ²²
Bank of England and FCA DP5/22	Feedback statement FS2/23 (October 2023) ²³
IMDA Model AI Governance Framework (2020) for agents	IMDA Model AI Governance Framework for Agentic AI, v1.5 (May 2026) ¹⁹
OWASP Top 10 for LLM Applications (2023)	2025 edition ¹²
OWASP Low-Code/No-Code Top 10	Related newer list: OWASP Citizen Development Top 10 (OWASP hasn't confirmed it as the successor) ¹¹
PCI DSS 4.0	PCI DSS 4.0.1 ¹⁰
EU AI Act "Title III"	Chapter III (high-risk AI systems); see the EU AI Act page

Questions to ask your counsel

1. Which frameworks are we contractually committed to (SOC 2, ISO/IEC 27001, PCI DSS), and do those commitments reach worker-built apps?
2. Do any customer contracts or public statements say we "comply with" a voluntary framework, and should we reword them?
3. Do we want ISO/IEC 42001 certification, or is a mapped alignment enough for our customers and regulators?
4. Which accessibility standard (WCAG 2.1 or 2.2 AA) do the laws that apply to us reference, and for which apps?
5. If we train or fine-tune models, which parts of SP 800-218A and the AI 600-1 profile should our contracts and policies adopt?

Assumptions and evidence

- This page relies on no register assumption. Control IDs for the paid ISO standards and the gated AICPA criteria come from published control lists and a third-party copy, not the purchased texts.
- Evidence: standards bodies' own publications, read on 2026-10-21 or 2026-10-22. The OWASP Citizen Development list has no stated version, its project page was unreliable, and its items were read from the project's source repository. The ISO pages refused automated fetches. The PCI DSS publication date comes from secondary sources.
- Facts on this page are as of October 2026.

Related

- [Compliance for vibe-coded apps](#): SOC 2 scoping, audit evidence and the claims register.
- [US and Canadian laws for AI-built apps](#): the legal obligations behind the frameworks.
- [Secure vibe coding: a review checklist](#): the build controls in practice.
- [MCP security for business AI tools](#): the agent and MCP rows in practice.

- [Risk tiers for worker-built apps](#): the gates the reuse table maps.

-
1. NIST, AI Risk Management Framework 1.0 (NIST AI 100-1), Jan 2023, under revision as of October 2026, <https://www.nist.gov/itl/ai-risk-management-framework> [primary], accessed 2026-10-21.
 2. NIST, AI 600-1, Generative Artificial Intelligence Profile, 26 Jul 2024, <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf> [primary], accessed 2026-10-21.
 3. NIST, The NIST Cybersecurity Framework (CSF) 2.0, CSWP 29, 26 Feb 2024, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf> [primary], accessed 2026-10-22.
 4. NIST, IR 8596 (initial preliminary draft), Cyber AI Profile, 16 Dec 2025, <https://csrc.nist.gov/pubs/ir/8596/iprd> [primary], accessed 2026-10-22.
 5. NIST, SP 800-218 v1.1, Secure Software Development Framework, Feb 2022, <https://csrc.nist.gov/pubs/sp/800/218/final>; SP 800-218 Rev. 1 initial public draft, 17 Dec 2025 (comments closed 30 Jan 2026; no final as of 2026-10-22), <https://csrc.nist.gov/pubs/sp/800/218/r1/ipd> [primary], accessed 2026-10-22.
 6. NIST, SP 800-218A, Secure Software Development Practices for Generative AI and Dual-Use Foundation Models, 26 Jul 2024, <https://csrc.nist.gov/pubs/sp/800/218/a/final> [primary], accessed 2026-10-22.
 7. ISO, ISO/IEC 42001:2023, AI management systems, <https://www.iso.org/standard/81230.html> [standard], accessed 2026-10-21.
 8. ISO, ISO/IEC 27001:2022, Information security management systems, <https://www.iso.org/standard/27001> [standard; paid text], accessed 2026-10-22.
 9. AICPA, 2017 Trust Services Criteria (With Revised Points of Focus, 2022), <https://www.aicpa-cima.com/resources/download/2017-trust-services-criteria-with-revised-points-of-focus-2022> [standard; free registration required], accessed 2026-10-21.
 10. PCI Security Standards Council, PCI DSS v4.0.1, document library, https://www.pcisecuritystandards.org/document_library/ [standard; the 11 Jun 2024 publication date and the end-2024 retirement of v4.0 come from secondary summaries, for example <https://secureframe.com/blog/pci-dss-4.0.1>, vendor], accessed 2026-10-22.
 11. OWASP, Citizen Development Top 10, source repository (no version stated; content path dated 2022), <https://github.com/OWASP/www-project-citizen-development-top10-security-risks> [primary]; project page <https://owasp.org/www-project-citizen-development-top10-security-risks/> (unreliable when checked), accessed 2026-10-21.
 12. OWASP, Top 10 for LLM Applications, 2025 edition, <https://genai.owasp.org/llm-top-10/> [primary], accessed 2026-10-21.
 13. OWASP, Top 10 for Agentic Applications for 2026, released 9 Dec 2025, <https://genai.owasp.org/resource/owasp-top-10-for-agentic-applications-for-2026/> [primary; the item names were confirmed through secondary sources], accessed 2026-10-22.
 14. Model Context Protocol, specification 2026-07-28 and security best practices, https://modelcontextprotocol.io/specification/2026-07-28/basic/security_best_practices [primary], accessed 2026-10-21.
 15. SLSA, "What's new in SLSA v1.2", <https://slsa.dev/spec/v1.2/whats-new> [primary], accessed 2026-10-21.
 16. OpenSSF Best Practices and AI/ML Working Groups, Security-Focused Guide for AI Code Assistant Instructions, 1 Aug 2025, <https://best.openssf.org/Security-Focused-Guide-for-AI-Code-Assistant-Instructions> [primary], accessed 2026-10-21.
 17. W3C, Web Content Accessibility Guidelines (WCAG) 2.2, <https://www.w3.org/TR/WCAG22/>; What's new in WCAG 2.2, <https://www.w3.org/WAI/standards-guidelines/wcag/new-in-22/> [primary], accessed 2026-10-22.
 18. CISA, Secure by Design, <https://www.cisa.gov/securebydesign> [regulator], accessed 2026-10-22.
 19. IMDA (Singapore), Model AI Governance Framework for Agentic AI, v1.5, May 2026, <https://www.imda.gov.sg/-/media/imda/files/about/emerging-tech-and-research/artificial-intelligence/mgf-for-agentic-ai.pdf> [regulator], accessed 2026-10-22.

20. 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.
21. 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.
22. 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.
23. Bank of England, PRA and FCA, FS2/23, Artificial Intelligence and Machine Learning, Oct 2023, <https://www.bankofengland.co.uk/prudential-regulation/publication/2023/october/artificial-intelligence-and-machine-learning> [regulator], accessed 2026-10-22.

Prompt to Prototype, Standards crosswalk for worker-built apps, <https://prompt-to-prototype.com/governance/standards/>, as of 2026-10-22. Licensed [CC BY-SA 4.0](#).