PANDORA CLOUD
UNPACKING COMPLEXITY

Fintech Compliance Crosswalk

One control set, five frameworks: SOC 2, PCI DSS, GLBA, NYDFS 500, and SOX ITGC mapped for fintech SMBs

A Pandora Cloud Buyer's Resource

September 2026

Pandora Cloud LLC
Women-Owned Small Business (WOSB) | AWS Advanced Partner
GSA MAS: 47QTCA24D00D3 | CAGE: 9JSG7 | UEI: R36GQ3N4XT63
Secret Facility Clearance | pandoracloud.net

About This Crosswalk

For a fintech, a System and Organization Controls 2 (SOC 2) report is rarely the finish line. It is the front door to a stack of overlapping obligations: the Payment Card Industry Data Security Standard (PCI DSS) if you touch cardholder data, the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule if you are a non-bank financial institution, New York Department of Financial Services (NYDFS) regulation 23 New York Codes, Rules and Regulations (NYCRR) Part 500 if you hold a New York license, and Sarbanes-Oxley Act (SOX) information technology general controls (ITGC) if you are public or your service affects a customer's financial reporting. Each arrives from a different buyer or regulator, on a different clock, with its own vocabulary.

The trap is treating each one as a separate program: implementing the same control three or four times, writing near-identical policies for each, and maintaining redundant evidence packages. The escape is recognizing that all five frameworks test the same underlying controls. Encryption, access control, logging, change management, and incident response show up in every one. Implement each control once, map it across the frameworks, and produce framework-specific evidence views from the same work.

This crosswalk is that map. It is built for compliance owners, security leads, and operations leaders at fintech small and mid-sized businesses (SMBs) under 200 people. Use it to plan a single control program that satisfies every framework your buyers and regulators demand, and to stop rebuilding from scratch each time a new one lands.

How to read the citations

Each cell points to the clause in that framework the control helps satisfy. Citations are current as of September 2026 (PCI DSS v4.0.1, NYDFS Part 500 Second Amendment, the GLBA Safeguards Rule at 16 Code of Federal Regulations (CFR) Part 314 as amended in 2021 (key provisions in force June 9, 2023) and 2023 (breach notification at 314.4(j), in force May 13, 2024), and the American Institute of Certified Public Accountants (AICPA) Trust Services Criteria (TSC) 2017/2022). Frameworks change; confirm every citation against the current published text, and have counsel or your assessor review scope before you rely on this for an audit.

Why Fintech Compliance Compounds

A law firm that clears one SOC 2 contract gate is usually safe across its book. A fintech that clears one is facing three more variants from three more counterparties inside eighteen months. Three forces drive that compounding.

Enterprise and banking partners stack requirements

A banking partner asks for a SOC 2 Type II report, a PCI DSS Attestation of Compliance (AOC), and quarterly evidence exports. A Fortune 500 customer adds a rider requiring semi-annual audit refreshes. A payments processor requires its own security review. Each counterparty assumes its questionnaire is the only one you answer; in aggregate they demand continuous, multi-framework evidence.

Regulators overlap and enforce

The GLBA Safeguards Rule (amended in 2021, with key provisions effective June 2023) now prescribes specific technical controls for non-bank financial institutions. NYDFS 23 NYCRR 500, after its 2023 Second Amendment, requires universal multi-factor authentication (MFA) and a documented asset inventory (both in force November 1, 2025) and, for Class A companies, endpoint detection and centralized logging. The Department enforces it: PayPal and Healthplex each paid $2 million in 2025 for MFA gaps, and National Securities Corporation paid $3 million in 2021 for MFA failures and unreported incidents. These regimes test the same underlying controls SOC 2 and PCI DSS already test.

The cost is in the duplication, not the controls

Most fintechs do not fail because a control is missing. They burn budget implementing encryption once for the SOC 2 auditor, again for the PCI assessor, and a third time for the NYDFS examiner, each with its own policy document and evidence folder. The control was the same every time. The waste was treating the frameworks as unrelated.

The Five Frameworks at a Glance

Before the crosswalk, a one-line orientation on each framework: who asks for it, what it governs, and whether it applies to you.

Framework	Who asks for it	What it governs	Applies when
SOC 2	Enterprise buyers, banks, procurement teams	Operational controls across the AICPA Trust Services Criteria (Security required; Availability, Processing Integrity, Confidentiality, Privacy optional)	You sell software or data services to enterprises
PCI DSS v4.0.1	Card networks, acquiring banks, payment partners	Protection of cardholder data across 12 requirement families	You store, process, or transmit cardholder data, or your service can affect its security
GLBA Safeguards (16 CFR 314)	The Federal Trade Commission (FTC)	Information security program for non-bank financial institutions	You are a non-bank financial institution handling customer financial information
NYDFS 500 (23 NYCRR 500)	New York Department of Financial Services	Cybersecurity program for NYDFS-licensed entities	You hold a NYDFS license or authorization

Framework	Who asks for it	What it governs	Applies when
SOX ITGC	External auditors, the Securities and Exchange Commission (SEC)	IT general controls supporting financial-reporting integrity	You are public, or your service affects a client's financial statements (SOC 1 territory)

SOX ITGC is organized into four control domains that external auditors conventionally test, rather than numbered clauses: APD (Access to Programs and Data), PC (Program Changes), PD (Program Development), and CO (Computer Operations). The crosswalk uses those abbreviations. "Entity-level" denotes controls assessed above the ITGC layer.

How to Use This Crosswalk

- **Identify your in-scope frameworks** from the table above. Most fintechs land on SOC 2 plus one or two others; a New-York-licensed payments company can hit all five.
- **Read down the control column, not across the framework columns.** The point is that one control implementation earns citations in every framework you are in scope for. Build the control once, to the strictest standard among your frameworks.
- **Produce framework-specific evidence views from the same control.** One access-review process generates the SOC 2 CC6 evidence, the PCI Req 7 evidence, and the NYDFS 500.7 evidence. You run it once; you export it three ways.
- **Sequence by your nearest deadline** (see "Sequence, Don't Stack"), implement against the unified catalog, then satisfy later frameworks as overlays rather than restarts.

The Crosswalk

Each row is one control from the unified catalog. Each cell is the clause that control helps satisfy in that framework. "n/a" means the framework does not test that control directly. Where a parent requirement is cited, the listed sub-requirement is the one an assessor tests first.

Control	SOC 2 (TSC)	PCI DSS v4.0.1	GLBA 314.4	NYDFS 500	SOX ITGC
Access and Identity					
Multi-factor authentication	CC6.1	8.4.2, 8.5.1	(c)(5)	500.12	APD
Role-based access / least privilege	CC6.1, CC6.3	7.2.1, 7.2.2, 7.3.1	(c)(1)	500.7	APD
Periodic access reviews	CC6.2, CC6.3	7.2.4	(c)(1)	500.7(a)(4)	APD
Unique IDs, provisioning / deprovisioning	CC6.1, CC6.2	8.2.1, 8.2.4	(c)(1)	500.7(a)(6)	APD
Data Protection					
Encryption at rest	CC6.1	3.5.1	(c)(3)	500.15	APD
Encryption in transit	CC6.7	4.2.1	(c)(3)	500.15	APD
Secure disposal / data retention	CC6.5; C1.1, C1.2	3.2.1, 9.4.6	(c)(6)	500.13(b)	CO
Logging and Monitoring					
Audit logging	CC7.2	10.2	(c)(8)	500.6	CO
Log review / analysis	CC7.2	10.4.1, 10.4.1.1	(c)(8)	500.14(a)(1)	CO
Continuous monitoring / anomaly detection	CC7.1, CC7.2	10.7.2, 11.5.1	(d)	500.14	CO
Vulnerability and Change					
Vulnerability scanning	CC7.1	11.3.1, 11.3.2	(d)(2)	500.5(a)(2)	CO
Penetration testing	CC4.1, CC7.1	11.4.1 to 11.4.3	(d)(2)	500.5(a)(1)	n/a
Change management	CC8.1	6.5.1	(c)(7)	500.3(i), 500.8	PC
Secure software development life cycle (SDLC)	CC8.1	6.2.1	(c)(4)	500.8	PD
Governance, Risk, and Resilience					
Risk assessment	CC3.1 to CC3.4	12.3.1 (targeted)	(b)	500.9	Entity-level
Vendor / third-party risk	CC9.2	12.8	(f)	500.11	CO / SOC 1
Incident response	CC7.3 to CC7.5	12.10.1	(h)	500.16(a)(1)	CO

Control	SOC 2 (TSC)	PCI DSS v4.0.1	GLBA 314.4	NYDFS 500	SOX ITGC
Business continuity / backup and recovery	A1.2, A1.3	12.10.1	(h)	500.16(a)(2), (e)	CO
Security awareness training	CC2.2	12.6.1	(e)	500.14(a)(3)	Entity-level
Program governance / named owner	CC1.1 to CC1.3	12.1, 12.4	(a), (i)	500.3, 500.4	Entity-level

GLBA citations are subsections of 16 CFR 314.4. NYDFS citations are sections of 23 NYCRR Part 500. PCI citations are requirement numbers in PCI DSS Requirements and Testing Procedures v4.0.1. SOC 2 citations are AICPA Trust Services Criteria; the Availability (A) and Confidentiality (C) criteria apply only when included in your report scope.

One Control, Five Attestations

Take multi-factor authentication, the single most-cited control across all five frameworks. A fintech that implements MFA once, correctly, and captures the evidence once earns credit in every regime it is subject to:

Framework	Clause	What that framework wants to see
SOC 2	CC6.1	MFA enforced on logical access to in-scope systems, evidenced across the audit window
PCI DSS	8.4.2, 8.5.1	MFA for all non-console access into the cardholder data environment, resistant to replay
GLBA	314.4(c)(5)	MFA for any individual accessing any information system, unless the Qualified Individual approves an equivalent control in writing
NYDFS 500	500.12	MFA for any individual accessing any information system of the covered entity; Chief Information Security Officer (CISO)-approved compensating controls must be reviewed at least annually
SOX ITGC	APD	Authentication control supporting access to financially-relevant programs and data

One implementation. One evidence artifact (the enforcement policy plus a configuration export and a sample of authentication logs). Five citations. The team that internalizes this stops asking "which MFA does the PCI assessor want" and starts asking "does our MFA meet the strictest standard among our frameworks," because meeting the strictest satisfies the rest.

Sequence, Don't Stack

You cannot implement five frameworks at once, and you should not try. Lead with the one tied to your nearest revenue or license deadline, build the unified control set to its standard, then layer the others as overlays. A rough sequencing guide by fintech type:

If you are a...	Lead with	Because
B2B fintech / SaaS platform selling to enterprises	SOC 2 Type II	It is the near-universal procurement gate; most other frameworks reuse its controls
Payments company touching card data	PCI DSS v4.0.1	Acquirers and payment partners require annual validation (a Self-Assessment Questionnaire (SAQ), or a Report on Compliance (ROC) led by a Qualified Security Assessor (QSA) at Level 1) with an AOC; scope is set by the standard, not negotiated
Lender, mortgage broker, or other non-bank financial institution under FTC jurisdiction (SEC-registered advisers and broker-dealers follow Regulation S-P instead)	GLBA Safeguards	It is a legal obligation, not a contract term, and applies whether or not a buyer asks
NYDFS-licensed entity (money transmitter, insurer, lender)	NYDFS 500	An active regulator enforces it with penalties; the April 15 annual certification is mandatory
Public company or SOC 1 service provider	SOX ITGC	Your financial-statement audit depends on it and the timeline is fixed by your fiscal year

Whatever you lead with, build against the unified catalog on the prior page. When the second framework's questionnaire arrives, the honest answer is "we already do that, here is the evidence in your format," not "give us a quarter."

Clocks, Certifications, and Thresholds

The crosswalk tells you which controls overlap. This table covers what does not overlap: the notification deadlines, the annual attestation each framework expects, and the thresholds that decide whether a framework applies to you at all.

Framework	Notification clock	Annual attestation and who signs	Applicability thresholds
SOC 2	No regulatory clock; incident communication follows your commitments (CC7.4)	Type II report each audit period, opinion issued by the CPA firm	Contractual; scope set by the criteria you include
PCI DSS	Notify the payment brands and acquirer per your 12.10.1 plan	AOC annually, signed by an executive officer (plus the QSA for a ROC)	Merchant Level 1 (over 6 million transactions a year) needs a QSA-led ROC; Levels 2 to 4 use an SAQ at acquirer discretion; service providers over 300,000 transactions need a ROC
GLBA Safeguards	Notice to the FTC within 30 days for events affecting 500 or more consumers (314.4(j), since May 13, 2024)	Qualified Individual's written report to the board at least annually (314.4(i))	Institutions with fewer than 5,000 consumers are exempt from the written risk assessment, annual penetration test, incident response plan, and board report (314.6)

Framework	Notification clock	Annual attestation and who signs	Applicability thresholds
NYDFS 500	72 hours to DFS for a cybersecurity incident (500.17(a)); 24 hours for an extortion payment plus a 30-day explanation (500.17(c))	Certification of material compliance by April 15, signed by the highest-ranking executive and the CISO (500.17(b)); records kept five years	Limited exemption (500.19(a)) below 20 employees, $7.5 million revenue, or $15 million assets; MFA still applies. Class A ($20 million New York revenue with 2,000 employees, or $1 billion revenue) adds an independent audit, endpoint detection, and central logging
SOX ITGC	Public companies: SEC Form 8-K Item 1.05 within four business days of a material-incident determination	Sections 302 and 404 management assessment each fiscal year, signed by the CEO and CFO	Public companies; service providers through the SOC 1 report the client's auditor relies on

Recurring tests the frameworks name explicitly

- Vulnerability scans: quarterly internal and external Approved Scanning Vendor (ASV) scans under PCI DSS 11.3.1 and 11.3.2; at least every six months under GLBA 314.4(d)(2); periodic and risk-based under NYDFS 500.5(a)(2).
- Penetration tests: annually under PCI DSS 11.4, GLBA 314.4(d)(2), and NYDFS 500.5(a)(1) (internal and external).
- Access reviews: every six months under PCI DSS 7.2.4; at least annually under NYDFS 500.7(a)(4).
- Risk assessment: at least annually under NYDFS 500.9; whenever the environment changes under GLBA 314.4(b).
- Incident response and business continuity: annual plan tests, including a restore-from-backup test, under NYDFS 500.16(d).
- Log retention: 12 months with 3 months immediately available under PCI DSS 10.5.1; five years for records supporting financial transactions and three years for security event logs under NYDFS 500.6(b).

Cost Expectations

The single-framework approach multiplies cost; the crosswalk approach compresses it. Honest ranges for an SMB fintech, and what moves them.

The duplication tax (what stacking costs)

Run separately, each framework carries its own audit or assessment fee, its own policy set, and its own evidence effort. A fintech pursuing SOC 2, PCI DSS, and one regulatory regime independently commonly spends a third to double what a unified control set costs over the first two years, mostly in duplicated internal hours and redundant tooling. Pandora Cloud's own modeling of a three-framework fintech stack (SOC 2, PCI DSS, GLBA) puts the standalone path 30 to 110 percent above a unified build in year one.

Typical SMB fintech ranges (unified approach)

- **SOC 2 Type II audit (Security only):** $25,000 to $60,000; add 15 to 25 percent per additional Trust Services Criterion.
- **PCI DSS validation:** SAQ path for smaller merchants; a QSA-led ROC runs materially higher and scales with cardholder-data-environment complexity.
- **GLBA / NYDFS:** no external audit fee in the SOC 2 sense, but real internal cost for the written program, the testing regime, the Qualified Individual's annual board report under GLBA, and the April 15 certification under NYDFS.
- **Continuous-monitoring tooling:** $5,000 to $30,000 per year, cloud-native at the low end, compliance-automation platform at the high end.

What pushes it up, and how to hold it down

Cost rises with cardholder-data-environment sprawl, multi-cloud complexity, and adding every optional criterion at once. It falls when you scope tightly, build one control set to the strictest standard, automate evidence collection from day one, and phase optional criteria to when a contract actually requires them.

Common Pitfalls

1. Treating each framework as a fresh project

The most expensive mistake. It produces three encryption policies, three access-review processes, and three evidence folders for what is one control. Map first, implement once.

2. Building to the weakest standard, then patching

If you implement MFA to satisfy SOC 2 and later discover PCI requires it on all non-console cardholder data environment (CDE) access, you rebuild. Build every shared control to the strictest standard among your in-scope frameworks the first time.

3. Ignoring the frameworks that do not send questionnaires

GLBA and NYDFS are legal obligations that apply whether or not a customer asks. Fintechs that only chase buyer-driven SOC 2 discover the regulatory obligations during an examination, which is the worst time.

4. Evidence that maps to one framework's format only

If your evidence is organized for the SOC 2 auditor alone, the PCI assessor and NYDFS examiner each trigger a reformatting scramble. Capture evidence once, tagged to the control, and export per framework.

5. Letting SOX ITGC scope creep silently

If you go public or sign a customer whose financial reporting depends on your service, SOX ITGC obligations attach to the same access, change, and operations controls you already run. Recognize the trigger before the external auditor does.

Where to Go From Here

This crosswalk sits alongside the rest of Pandora Cloud's compliance toolkit. Depending on where you are:

- **If you need the controls running continuously:** the Continuous Monitoring Toolkit gives you 25 controls to monitor across five areas, with copy-paste setup walkthroughs for the highest-impact ones on Amazon Web Services (AWS), Azure, and Google Cloud. Free at pandoracloud.net/continuous-monitoring-toolkit/.
- **If you need the operating program around the controls:** the Compliance Program Blueprint lays out the month-by-month cadence, roles, and evidence rhythm that keeps every framework current between audits. Free at pandoracloud.net/compliance-program-blueprint/.
- **If SOC 2 is your lead framework:** the SOC 2 Readiness Checklist scores your readiness and maps the 90-day path to audit kickoff. Free at pandoracloud.net/soc2-readiness-checklist/.
- **To model the cost:** the Cost Calculator compares building compliance in from the start versus catching up under a procurement clock. pandoracloud.net/cost-calculator/.

A Note on Pandora Cloud

Pandora Cloud is a Women-Owned Small Business and an Amazon Web Services (AWS) Advanced Tier Partner with a Defense Counterintelligence and Security Agency (DCSA) Secret-level Facility Clearance and Cybersecurity Maturity Model Certification (CMMC) Level 2 self-assessment status. We help regulated SMBs across finance, healthcare, legal, insurance, and defense build audit-ready cloud environments and operate them as part of normal business, not as periodic audit projects.

If you are staring at a stack of frameworks and trying to work out which controls overlap and which order to tackle them in, that is exactly the conversation we have with fintech founders every week.

See what a multi-framework program actually costs for a firm your size: pandoracloud.net/cost-calculator/. Compare the cost of building the control set in from the start versus catching up under a 60-day procurement clock.

Want a second set of eyes on your framework stack?

Schedule a free 30-minute consultation. We will map your in-scope frameworks to a single control set and help you sequence the next 90 days.

pandoracloud.net/#schedule-consultation

Glossary

For readers new to the vocabulary, this glossary names the most common terms referenced in this crosswalk.

AOC (Attestation of Compliance): The signed declaration of PCI DSS compliance status, the artifact a payment partner asks to see.

CDE (Cardholder Data Environment): The systems that store, process, or transmit cardholder data; the scope boundary for PCI DSS.

GLBA Safeguards Rule (16 CFR Part 314): The FTC rule requiring non-bank financial institutions to maintain an information security program with prescribed technical controls.

ITGC (IT General Controls): The access, change, development, and operations controls that support the reliability of financially-relevant systems under SOX.

NYDFS 500 (23 NYCRR Part 500): The New York Department of Financial Services cybersecurity regulation for licensed entities, materially amended in 2023.

Nonpublic Information (NPI): The protected-data category under NYDFS 500. GLBA's Privacy Rule uses the near-identical term "nonpublic personal information"; the Safeguards Rule scopes it as "customer information."

SOC 1 vs SOC 2: SOC 1 covers controls over financial reporting (relevant to SOX reliance); SOC 2 covers operational security controls against the Trust Services Criteria.

SOX (Sarbanes-Oxley): The law requiring public companies to attest to internal controls over financial reporting, which depend on IT general controls.

Trust Services Criteria (TSC): The AICPA criteria a SOC 2 report is evaluated against: Security (required), Availability, Processing Integrity, Confidentiality, Privacy.

Type II report: A SOC 2 report testing whether controls operated effectively across an observation window, typically 6 to 12 months, not just at a point in time.