



7T World

Global Innovation, Anchored in Trust

The Payments Compliance Automation Framework

An Executive Overview

How leading institutions map compliance controls across
18 payment channels and 15 major regulations.

18

Payment Channels

512

Compliance Controls

15

Regulations

96.4%

Compliance Rate

The Payments Compliance Challenge

Today's payment ecosystem spans traditional cards and ACH, digital wallets and peer-to-peer transfers, real-time payments, cryptocurrency, buy-now-pay-later, and cross-border remittances. Each channel carries its own risk profile and regulatory obligations — and the complexity is accelerating.

Financial institutions face an expanding web of regulations: PCI-DSS for card data security, BSA/AML and OFAC for financial crime prevention, NACHA rules for ACH networks, Reg E and Reg Z for consumer protection, GDPR for data privacy, and emerging frameworks for cryptocurrency and real-time payments. Managing compliance across all of these simultaneously — with manual processes — is no longer tenable.

■ **Organizations managing 10+ payment channels report spending an average of 2,400+ hours annually on compliance activities. Automation can reduce this by 60–75%.**

What This Framework Provides

The 7T World Payments Compliance Automation Framework is a structured approach to mapping every payment channel your institution operates to the specific regulatory requirements, risk controls, and testing procedures that apply. It replaces spreadsheet-based tracking with a systematic, auditable, and automatable methodology.

- ✓ A complete taxonomy of 18 payment channel types with risk classifications
- ✓ Pre-mapped regulatory requirements across 15 major U.S. and international regulations
- ✓ A risk scoring methodology that weights volume, regulatory complexity, and fraud exposure
- ✓ Testing schedules calibrated to risk level — monthly for critical controls, quarterly to annual for standard ones
- ✓ Audit preparation workflows with 30-day, 14-day, and 7-day readiness checklists

Payment Channel Risk Taxonomy

The framework organizes payment channels into five categories, each with distinct risk characteristics, regulatory requirements, and control priorities.

CATEGORY	CHANNELS	RISK	KEY REGULATIONS
Card-Based Payments	Credit Cards, Debit Cards, Prepaid Cards	HIGH	PCI-DSS, Reg Z, Reg E, EMV, 3-D Secure
Bank Transfers	ACH (Debit/Credit), Domestic Wires, International Wires	HIGH	BSA/AML, OFAC, NACHA, Reg E, SWIFT/Fedwire
Digital Wallets	Apple Pay, Google Pay, PayPal, Venmo, P2P	MEDIUM	Reg E, State MTL, PCI-DSS, GLBA
Real-Time & Crypto	FedNow, RTP Network, Bitcoin, Stablecoins	HIGH	BSA/AML, OFAC, FFIEC, State DLT Regulations
BNPL & Cross-Border	Affirm, Afterpay, Klarna, Remittance Services	MEDIUM	Reg Z, TILA, CFPB, OFAC, State MTL

Risk Scoring Methodology

Each channel is scored across four dimensions, weighted to reflect enterprise risk priorities:

$$\text{Risk Score} = (\text{Volume Score} \times 0.30) + (\text{Regulatory Complexity} \times 0.30) + (\text{Fraud Risk} \times 0.20) + (\text{Operational Complexity} \times 0.20)$$

Channels scoring above 7.5 are classified as High Risk and require monthly or quarterly control testing. Channels between 4.0 and 7.5 are Medium Risk (semi-annual testing), and below 4.0 are Low Risk (annual testing). These thresholds are configurable to match your institution's risk appetite.

Regulatory Coverage Reference Map

The framework maps 15 major regulations to the payment channels where they apply, ensuring no regulatory gap goes unaddressed.

REGULATION	SCOPE	APPLIES TO	KEY REQUIREMENTS
PCI-DSS	Card Data Security	Cards, Wallets, E-commerce	Quarterly vuln scans, annual pen tests, encryption, access controls, segmentation
BSA/AML	Financial Crime	All Channels	CDD/EDD, transaction monitoring, SAR filing, CTR reporting, annual testing
OFAC	Sanctions Compliance	Wires, Crypto, Cross-Border	Real-time screening, SDN list updates, 50% rule, blocked transactions reporting
NACHA	ACH Network	ACH Debit/Credit, Same-Day ACH	Return rate monitoring (<1%/15%), authorization, third-party sender due diligence
Reg E	Consumer Protection	Debit, ACH, P2P, Wallets, RTP	Error resolution, unauthorized transfer liability, disclosure requirements
Reg Z / TILA	Lending Disclosure	Credit Cards, BNPL	APR disclosure, billing dispute rights, ability-to-repay assessment
GDPR	Data Privacy	All Channels (EU customers)	Consent management, data minimization, right to erasure, breach notification (72hr)
FFIEC	IT Examination	All Channels	IT risk assessment, business continuity, cybersecurity framework, vendor management

Additional regulations covered in the full framework include SOX (financial controls), GLBA (data protection), FCRA (credit reporting), State Money Transmitter Licenses, PSD2 (EU payment services), CCPA (California privacy), and MAS Guidelines (Singapore).

Audit Preparation Timeline

Regulatory examinations require systematic preparation. The framework includes a structured countdown that ensures readiness without last-minute scrambling.

■ 30 DAYS BEFORE

- ✓ Run comprehensive compliance check across all payment channels
- ✓ Review and resolve all high-risk findings from prior testing cycles
- ✓ Update control documentation with current procedures and evidence
- ✓ Verify all control owners are current and responsibilities are documented
- ✓ Confirm testing coverage meets minimum thresholds by risk tier

■ 14 DAYS BEFORE

- ✓ Export complete audit package with executive summary
- ✓ Review findings and remediation status with legal/compliance team
- ✓ Prepare evidence documentation for each tested control
- ✓ Validate that all regulatory mapping is current (new rules, amendments)
- ✓ Brief control owners on potential examiner questions and evidence locations

■ 7 DAYS BEFORE

- ✓ Final testing validation — confirm no new overdue items
- ✓ Update executive dashboard with current KPIs and trend data
- ✓ Prepare presentation materials for examiner opening conference
- ✓ Stage all evidence in accessible, organized repository
- ✓ Conduct dry-run walkthrough with key stakeholders

Implementing the Framework

This executive overview describes the structure of the 7T World Payments Compliance Automation Framework. The full implementation includes 512 pre-mapped controls, automated testing schedules, real-time compliance dashboards, and regulatory change monitoring — configured to your institution's specific payment channels and risk profile.

Who This Serves

- **Banks and Credit Unions** — Comprehensive AML/OFAC compliance, card issuing and acquiring oversight, ACH and wire transfer monitoring across all business lines
- **Payment Processors** — Multi-merchant portfolio compliance, PCI-DSS and fraud prevention controls, payment channel risk aggregation
- **Fintechs** — Scalable compliance from startup to enterprise, multi-payment-method support, rapid adaptation to new regulatory requirements
- **E-commerce Platforms** — Multi-channel payment acceptance compliance, global regulatory coverage, third-party payment provider oversight

Request Your Custom Compliance Assessment

A 7T World specialist will evaluate your current compliance posture across your payment channels and deliver a prioritized action plan — no obligation.

7tworld.com/contact

Or email us directly at contact@7tworld.com

© 2026 7T World. All rights reserved. This document is provided for informational purposes. The compliance framework described herein should be adapted to each institution's specific regulatory requirements and risk profile. 7T World recommends consulting with legal and compliance counsel before implementation.