

TPRM REGULATORY REFERENCE GUIDE

Key Regulations, Frameworks, and Standards Affecting Third-Party Risk Management

Available at www.tpvrm.net/documents | *The Future of Third-Party Risk Management & Data Privacy*

This reference guide outlines the main regulatory frameworks and standards that establish third-party risk management obligations for organizations. It serves as a practical tool for TPRM practitioners, not as legal advice. Organizations should seek legal counsel for compliance requirements specific to their jurisdiction.

Note: Regulatory requirements change over time. Check current requirements against official regulatory sources. Last comprehensive review: June 2026.

DATA PRIVACY REGULATIONS

Regulation / Framework	Jurisdiction	Sector / Scope	TPRM Obligation	Key Provisions Affecting Vendor Contracts	Effective / Amended
GDPR	EU / EEA (global reach)	All sectors; EU personal data	Mandatory Data Processing Agreements (Art. 28). Controller must ensure processor provides sufficient guarantees. Prior authorization or notification for subprocessors. Data subject rights flow-down. Breach notification within 72 hours.	DPA required per Art. 28. SCCs for cross-border transfers. Processor audit rights. Subprocessor list maintenance. Data deletion/return at contract end.	May 2018
CCPA / CPRA	California, USA	For-profit businesses meeting thresholds; CA consumer data	Service provider agreements must prohibit selling/sharing personal information, require deletion at contract end, and restrict use to specified business purposes. Opt-out rights flow-down required.	Service Provider Contract required. Data use restrictions. Consumer rights assistance. Annual cybersecurity audit for some entities.	Jan 2020 / Jan 2023
HIPAA	USA	Healthcare covered entities and business associates	Business Associate Agreements (BAA) required for any vendor creating, receiving, maintaining, or transmitting PHI. BAA must require equivalent safeguards, breach notification, and PHI return/destruction.	BAA per 45 CFR 164.308(b). Minimum necessary standard. Breach notification: 60 days. Subcontractor BAA flow-down. Audit access rights.	Apr 2003; updated 2013
PIPEDA / Bill C-27	Canada	Private sector; personal information	Accountability for personal information transferred to third parties. Comparable privacy protection required by contract. Breach notification obligations.	Contractual protections comparable to PIPEDA. Breach notification and recordkeeping. Data use limitation clauses.	2001; Bill C-27 pending
Digital Personal Data Protection Act, 2023	India	Any organization processing personal data of	Data fiduciary obligations when engaging data processors; due diligence on processors; cross-border transfer restrictions;	Sections 7-9 (lawful processing grounds); Section 16 (cross-border transfers); Data Protection Board of	Enacted August 11, 2023; implementing rules

Regulation / Framework	Jurisdiction	Sector / Scope	TPRM Obligation	Key Provisions Affecting Vendor Contracts	Effective / Amended
(India)		Indian residents	contractual requirements for processors	India enforcement	expected 2024-2026

FINANCIAL SERVICES REGULATIONS

Regulation / Framework	Jurisdiction	Sector / Scope	TPRM Obligation	Key Provisions Affecting Vendor Contracts	Effective / Amended
DORA	EU / EEA	Financial entities (banks, insurers, investment firms, etc.) and ICT third-party service providers	Mandatory contractual requirements for ICT third-party services. Register of all ICT third-party arrangements. Concentration risk monitoring. Critical ITSP designation by ESMA/EBA/EIOPA. TLPT participation requirements.	Contractual clauses: full service description, audit rights, exit strategies, sub-outsourcing register, data location, ICT security requirements, business continuity provisions, incident reporting.	Jan 17, 2025
OCC Bulletin 2023-17	USA	National banks and federal savings associations	Third-party risk management guidance requiring due diligence, contract provisions, ongoing monitoring, and termination planning for all third-party arrangements, with heightened requirements for critical activities.	Written contracts covering accountability, performance measures, audit rights, confidentiality, business continuity, breach notification, dispute resolution, and termination rights.	Jun 2023
PCI DSS v4.0	Global	Entities storing, processing, or transmitting cardholder data	Assessment of all third-party service providers (TSPs) with access to cardholder data. Annual written acknowledgment of TSP responsibility for applicable PCI DSS controls. Validation of TSP compliance (AoC or equivalent).	TSP written acknowledgment (Req. 12.8). Monitoring of TSP PCI DSS status. Responsibility matrix. CDE segmentation verification for shared environments.	Mar 2022 (v4.0)
SEC Rule 38a-1 / Vendor Risk	USA	Registered investment advisers and funds	Due diligence on service providers. Written compliance policies and procedures. Annual review. Material change notification requirements for critical service providers.	Service provider due diligence documentation. Written agreements with compliance obligations. Material change notification.	Ongoing guidance

CYBERSECURITY AND TECHNOLOGY FRAMEWORKS

Regulation / Framework	Jurisdiction	Sector / Scope	TPRM Obligation	Key Provisions Affecting Vendor Contracts	Effective / Amended
NIST CSF 2.0	USA (global adoption)	All sectors; voluntary framework	Supply chain risk management integrated as "GV.SC" function. Identification of cybersecurity supply chain risks. Supplier assessments aligned with CSF tiers. Continuous monitoring of supply chain posture.	Supplier contracts aligned to CSF practices. Incident notification requirements. Software bill of materials (SBOM). Security requirements flow-down.	Feb 2024
NIST SP 800-161r1	USA	Federal agencies;	Comprehensive C-SCRM framework. Tiered risk	Supply chain risk assessment	May 2022

Regulation / Framework	Jurisdiction	Sector / Scope	TPRM Obligation	Key Provisions Affecting Vendor Contracts	Effective / Amended
		recommended for critical sectors	management: organization, mission/business process, and information system. Supplier screening, assessment, and monitoring.	requirements. Flow-down of security controls to suppliers. SBOM requirements. Provenance tracking for critical components.	
ISO 27001:2022	Global	All sectors; certification standard	Supplier relationships addressed in Annex A controls. Information security requirements for suppliers. Monitoring and reviewing supplier services. Supplier agreements with defined security requirements.	Supplier security policy. Supplier agreements with security requirements. ICT supply chain security. Monitoring and review of supplier service delivery.	Oct 2022
CMMC 2.0	USA	DoD contractors and subcontractors	Certification required to handle CUI (Level 2/3) or FCI (Level 1). C3PAO assessment for Level 2/3. Flow-down of CMMC requirements to subcontractors. Annual affirmation of compliance.	NIST 800-171 controls flow-down. Subcontract CMMC certification requirements. CUI handling restrictions. CMMC level specification in contracts.	2024
NIS2 Directive (Directive (EU) 2022/2555)	European Union	Critical infrastructure, essential and important entities across EU member states	Due diligence on ICT third-party providers; contractual security requirements for supply chain; mandatory incident reporting (24-hour early warning, 72-hour notification); supply chain risk assessments	Articles 20-21 (security requirements); Article 22 (supply chain security); enforcement by national competent authorities	October 17, 2024

ARTIFICIAL INTELLIGENCE REGULATIONS

Regulation / Framework	Jurisdiction	Sector / Scope	TPRM Obligation	Key Provisions Affecting Vendor Contracts	Effective / Amended
EU AI Act	EU / EEA (global reach)	All sectors; AI system providers, deployers, importers	Deployers of high-risk AI systems must ensure providers comply with Act requirements. Due diligence on AI system providers. Transparency and documentation requirements for high-risk AI. Register of high-risk AI systems.	Art. 26 deployer obligations: vendor AI system documentation, human oversight measures, fundamental rights impact assessments, incident reporting, data governance verification.	Aug 2024 (phased)
NIST AI RMF 1.0	USA (global reference)	All sectors; voluntary framework	AI risk management across MAP, MEASURE, MANAGE, and GOVERN functions. Third-party AI risk addressed in supply chain context. AI system documentation and transparency requirements.	AI system documentation requirements. Bias and fairness assessment. Model performance monitoring. AI incident reporting. Contractual AI governance provisions.	Jan 2023

Regulation / Framework	Jurisdiction	Sector / Scope	TPRM Obligation	Key Provisions Affecting Vendor Contracts	Effective / Amended
OMB M-24-10	USA	Federal agencies and their vendors	Minimum practices for federal agency AI governance. AI use case inventory. AI impact assessments. Third-party AI governance due diligence for federal procurement.	AI governance documentation for federal vendors. Safety and rights-impacting AI designation. Annual AI use case review. Human oversight requirements.	Mar 2024
ISO/IEC 42001:2023 - AI Management System	International (ISO standard, not a regulation)	Any organization developing or deploying AI systems	AI vendor governance; AI risk assessment requirements; audit rights for AI systems; transparency obligations; third-party AI controls and documentation	Clause 6 (planning and risk treatment); Clause 8 (operational controls); Annexes A and B (controls and guidance for AI-specific risks)	December 2023

HEALTHCARE SECTOR STANDARDS

Regulation / Framework	Jurisdiction	Sector / Scope	TPRM Obligation	Key Provisions Affecting Vendor Contracts	Effective / Amended
HIPAA Security Rule	USA	Covered entities and business associates	Security risk analysis required. Administrative, physical, and technical safeguards for ePHI. Business associate agreements with security obligations. Breach notification within 60 days.	45 CFR Part 164. BAA security requirements. Workforce security training. PHI access controls. Audit logging. Transmission security.	Apr 2005; updated 2013
HITRUST CSF	USA (global adoption)	Healthcare and cross-sector	HITRUST certification provides evidence of security control maturity. Third-party assurance program enables vendor risk assessment through standardized controls.	HITRUST r2 or e1 assessment. Control inheritance documentation. Third-party assurance leveraging. Annual recertification.	Ongoing revisions

GOVERNMENT AND DEFENSE

Regulation / Framework	Jurisdiction	Sector / Scope	TPRM Obligation	Key Provisions Affecting Vendor Contracts	Effective / Amended
FAR 52.204-21	USA	All federal contractors processing FCI	Basic safeguarding of covered contractor information systems. Minimum 15 security controls required. Flow-down to subcontractors who handle FCI.	Information system security plan. Access limitation to authorized users. Identification and authentication controls. Configuration management. Incident response.	Jun 2016
NIST SP 800-171r2	USA	Non-federal entities handling CUI	110 security requirements across 14 families. Required for DoD contractors pending	Full 110-control implementation. SSP documentation. POA&M for any open findings.	Feb 2020

Regulation / Framework	Jurisdiction	Sector / Scope	TPRM Obligation	Key Provisions Affecting Vendor Contracts	Effective / Amended
			CMMC. System Security Plan (SSP) and Plan of Action & Milestones (POA&M) required.	Annual self-assessment (or C3PAO for CMMC Level 2). CUI access controls.	

USING THIS GUIDE

Step 1: Determine which regulations apply to your organization based on sector, jurisdiction, and types of data handled.

Step 2: Cross-reference applicable regulations with your ITC scope assessment to determine which additional assessment modules are needed.

Step 3: Make sure vendor contracts contain the necessary provisions for each relevant regulation. Use the Contract Review Checklists (Artifact 06) to verify.

Step 4: Update this reference guide yearly or whenever significant regulatory changes happen. The regulatory requirements listed here are accurate as of 2025; always verify current requirements with legal counsel.

Last Reviewed By	
Review Date	
Next Review Due	