VendRisk360
ASSESS · MONITOR · STAY AHEAD

WHITEPAPER

The Global TPRM Regulatory Map: One Program for North America, Europe, Asia-Pacific and the Middle East

How multinational and cross-border firms can run one third-party risk program that satisfies regulators in every jurisdiction where they operate.

Published 25 September 2026

Written for Heads of TPRM, CROs, CISOs, compliance officers, internal audit and group risk functions

Online www.vendrisk360.com/resources/whitepapers/global-tprm-regulatory-map/

Contents

A practitioner map of third-party risk rules across the US, Canada, EU, UK, India, Singapore, the Philippines, the Middle East and Australia/NZ, with terminology and lifecycle crosswalks and one control set.

A bank with branches in New York, London and Singapore, a payments processor licensed in the EU and India, or an insurer with operations in Sydney and Riyadh all face the same practical problem. Each regulator has written its own third-party or outsourcing rulebook, each uses its own vocabulary, and each examiner expects to see evidence in its own shape. Firms that respond by building a separate program per country end up assessing the same cloud provider five times, keeping five inconsistent registers, and explaining to every examiner why the numbers do not match.

This paper maps the major regimes across North America, Europe, Asia-Pacific and the Middle East, shows where they converge and where they genuinely diverge, and sets out how to build one control set with local add-ons. It is a summary for practitioners, not legal advice. Rules, guidance and implementation timetables change; confirm current obligations with counsel and your supervisors before relying on any single statement here.

KEY TAKEAWAYS

- Most TPRM regimes share the same lifecycle: governance, inventory, risk assessment, due diligence, contracting, monitoring, incidents, concentration, exit and reporting.
- The differences that matter are mostly in terminology, register formats, regulator notification, data location and regulator access rights.
- A single global policy with short local annexes is easier to operate, test and defend than parallel country programs.
- Map one criticality scale to each local definition (critical activity, critical or important function, material outsourcing, material service provider) and record the mapping per vendor.
- Use NIST CSF 2.0, ISO/IEC 27001:2022 and SOC reports as the common technical baseline, then layer regulatory evidence on top.
- Treat the regulatory map itself as a controlled document with an owner, a review cadence and a change log.

Why multinationals need one program

Regulators increasingly look at the group, not just the local entity. A supervisor in Frankfurt or Toronto will ask how a critical provider is overseen at group level, whether the local register reconciles to the group inventory, and whether concentration is measured across the whole firm. Parallel programs make those questions hard to answer.

There are also operational reasons. Most material vendors (cloud platforms, core banking and card processors, payroll, customer communications, security tooling) serve several entities at once. Assessing them once, to the highest applicable standard, and reusing the evidence locally reduces

vendor fatigue and cost. It also produces one version of the truth about each vendor's risk, findings and remediation.

The goal is not to average the rules. It is to meet the strictest applicable requirement in the core program where that is cheap to do, and to isolate genuinely local obligations (a specific register template, a notification to a named authority, a data residency condition) in clearly owned annexes.

SCOPE OF THIS MAP

This paper focuses on prudential and conduct rules for financial institutions plus the sector and privacy overlays most regulated firms face (HIPAA, PCI DSS, GDPR and national data protection laws). Insurers, market infrastructures and payment institutions may have additional instruments. Check the text that applies to your license type.

Terminology crosswalk

Every regime draws a line between ordinary third-party arrangements and the ones that deserve the most scrutiny. The words differ, and the definitions are not identical, but the intent is similar: identify the arrangements whose failure would hurt customers, markets or the firm's ability to operate.

KEY TERMS BY REGIME

Term	Where it is used	What it signals
Third-party relationship	US interagency guidance; OSFI B-10 (third-party arrangement)	Any business arrangement, contractual or not
Critical activity	US interagency guidance	Activity whose failure could cause significant harm
Outsourcing	EBA guidelines, PRA SS2/21, RBI, MAS, BSP, SAMA, CBUAE	Provider performs a service the firm would otherwise do
Material outsourcing	PRA SS2/21, RBI, MAS, SAMA, CBUAE	Outsourcing with significant impact if it fails
ICT third-party service	DORA	Digital and data services provided on an ongoing basis
Critical or important function	DORA, EBA guidelines, FCA SYSC 8	Function whose disruption would materially impair the firm
Important business service	UK operational resilience	Service to clients whose disruption causes intolerable harm

Term	Where it is used	What it signals
Critical operation	APRA CPS 230	Process whose disruption has material impact on customers or the firm
Material service provider	APRA CPS 230	Provider the firm relies on for a critical operation or material risk
Business associate	HIPAA	Party handling protected health information for a covered entity
Processor	GDPR, UK GDPR, DPDP Act (data processor), Philippine DPA (personal information processor)	Party processing personal data on the controller's instructions
Third-party service provider	NYDFS Part 500, PCI DSS	Provider with access to covered systems or cardholder data

Two practical rules follow. First, keep one internal tier scale (for example Critical, Material, Low) and record for each vendor which local labels apply, rather than renaming your tiers per country. Second, recognize that labels are not interchangeable: a DORA critical or important function is assessed at function level, APRA critical operations at process level, and UK important business services from the client's point of view. One vendor can be critical under one lens and not under another.

North America

United States: banking agencies and FFIEC

The Interagency Guidance on Third-Party Relationships: Risk Management (June 2023; OCC Bulletin 2023-17, Federal Reserve SR 23-4, FDIC FIL-29-2023) is the anchor for banks. It describes a lifecycle of planning, due diligence and third-party selection, contract negotiation, ongoing monitoring and termination, supported by governance: oversight and accountability, independent reviews, and documentation and reporting. Oversight is expected to be risk-based and commensurate with the criticality of the activity, with heightened expectations for critical activities. The May 2024 guide for community banks translates this for smaller institutions.

The FFIEC IT Examination Handbook supplies the examination lens, particularly the Outsourcing Technology Services, Business Continuity Management, and Architecture, Infrastructure, and Operations booklets. Where vendors provide models, SR 11-7 and OCC 2011-12 model risk management guidance also apply.

United States: credit unions, NYDFS, health and payments

- NCUA guidance such as Letter to Credit Unions 07-CU-13 sets due diligence expectations. NCUA lacks direct examination authority over credit union service vendors, which places more

weight on the credit union's own oversight evidence.

- NYDFS 23 NYCRR Part 500, amended November 2023, requires covered entities to maintain a third party service provider security policy (section 500.11) covering identification, risk assessment, minimum practices, due diligence and periodic assessment.
- HIPAA requires business associate agreements with parties handling protected health information (45 CFR 164.502(e), 164.504(e) and 164.308(b)).
- PCI DSS v4.0 requirement 12.8 covers the list of third-party service providers, written agreements, due diligence, annual monitoring of compliance status and a responsibility matrix; 12.9 requires service providers to acknowledge their responsibilities to customers.

Canada: OSFI B-10

OSFI Guideline B-10 Third-Party Risk Management (final April 2023, effective May 1, 2024) applies to federally regulated financial institutions. It covers a broad set of third-party arrangements, not only outsourcing, and expects a risk-based framework across the lifecycle, including subcontractor risk, concentration, technology and cyber risk, and exit planning. It works alongside Guideline B-13 on technology and cyber risk and Guideline E-23 on model risk (check the effective date of the revised version).

Europe and the United Kingdom

European Union

DORA, Regulation (EU) 2022/2554, has applied since 17 January 2025. Its ICT third-party risk provisions require an ICT third-party risk strategy, a register of information on all contractual arrangements with ICT third-party service providers (distinguishing those supporting critical or important functions), reporting to competent authorities, a preliminary assessment of ICT concentration risk, key contractual provisions and exit strategies. Implementing technical standards define the register templates. The ESAs designate critical ICT third-party providers (CTPPs) for direct oversight, which does not relieve firms of their own responsibility.

- EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02) remain relevant for non-ICT outsourcing: critical or important functions, the outsourcing register, sub-outsourcing and exit plans. Check how your competent authority aligns them with DORA for ICT services.
- NIS2, Directive (EU) 2022/2555, lists supply chain security among the cybersecurity risk-management measures for essential and important entities, implemented through national transposition.
- GDPR Article 28 requires processor contracts, prior authorization for sub-processors and flow-down of obligations.

United Kingdom

PRA SS2/21 Outsourcing and third party risk management (effective 31 March 2022) covers material outsourcing and non-outsourcing third-party arrangements, expects a register, business continuity and exit planning, and requires notification of material outsourcing. FCA SYSC 8 applies to outsourcing of critical or important operational functions. The PRA and FCA operational resilience rules require firms to identify important business services, set impact tolerances and map the third parties that support them; the transition period ended in March 2025. The critical third parties regime under the Financial Services and Markets Act 2023, with rules in force from 1 January 2025, allows HM Treasury to designate providers for direct regulatory oversight.

Asia-Pacific and the Middle East

India

- The RBI Master Direction on Outsourcing of Information Technology Services (April 2023, effective 1 October 2023) requires a board-approved policy, materiality assessment, due diligence, concentration risk management, audit and access rights for the regulated entity and RBI, controls over sub-contracting, business continuity and exit.
- The RBI Master Direction on IT Governance, Risk, Controls and Assurance Practices (November 2023) sets board and management expectations that include third-party technology risk.
- SEBI's Cybersecurity and Cyber Resilience Framework (CSCRF, August 2024) includes third-party and vendor risk expectations for SEBI regulated entities, graded by entity category; check current implementation dates.
- The Digital Personal Data Protection Act 2023 distinguishes data fiduciaries and data processors. Check the status of implementing rules and phased commencement.

Singapore and the Philippines

MAS Guidelines on Outsourcing set expectations for material outsourcing arrangements, including risk assessment, due diligence, contract terms, audit and access for MAS, sub-contracting and exit. The MAS Technology Risk Management Guidelines (January 2021) include third-party management, and the MAS Notice on cyber hygiene sets baseline controls. The PDPA governs personal data handled by data intermediaries.

In the Philippines, BSP outsourcing rules in the Manual of Regulations for Banks and BSP IT risk management regulations govern service provider oversight, and the Data Privacy Act of 2012 covers personal information processors.

Middle East

In Saudi Arabia, the SAMA Rules on Outsourcing govern material outsourcing (with additional conditions for outsourcing outside the Kingdom), and the SAMA Cyber Security Framework includes a third-party cyber security domain. The Saudi PDPL covers personal data. In the UAE, the CBUAE Outsourcing Regulation and Standards for banks set expectations for material outsourcing, and the UAE PDPL applies to personal data. Both markets place weight on supervisory engagement before material or offshore arrangements; check current approval or notification requirements.

Australia and New Zealand

APRA CPS 230 Operational Risk Management (effective 1 July 2025) requires identification of critical operations and tolerance levels, management of material service providers, a register of material arrangements, notification to APRA of material arrangements and offshoring, and attention to the fourth parties a material service provider relies on. CPG 230 provides guidance. CPS 234 Information Security requires firms to assess the information security capability of third parties managing their information assets and to test control effectiveness. In New Zealand, the RBNZ outsourcing policy (BS11) applies to relevant registered banks and focuses on the ability to continue basic functions if a provider fails.

Common denominators by lifecycle stage

Beneath the vocabulary, the regimes ask for the same ten capabilities. The three tables below summarize expectations by stage and regime cluster. Cells are summaries; the absence of an explicit requirement is not permission to skip a stage.

LIFECYCLE EXPECTATIONS (NORTH AMERICA, EU, UK)

Stage	US and Canada	EU (DORA, EBA)	UK (PRA, FCA)
Governance and policy	Board oversight, risk-based program	ICT third-party strategy, management body approval	Board-approved policy, accountable SMF
Inventory and register	Complete inventory with criticality	Register of information, prescribed templates	Outsourcing and third-party register
Planning and risk assessment	Planning before engagement	Pre-contract risk assessment	Materiality assessment
Due diligence	Scaled to criticality	Due diligence before contract	Proportionate due diligence
Contracting	Rights, audit, termination	Mandatory contractual provisions	Access, audit, sub-outsourcing terms
Ongoing monitoring	Performance, risk, independent review	Monitoring of provider performance	Ongoing oversight, testing

Stage	US and Canada	EU (DORA, EBA)	UK (PRA, FCA)
Incidents	Vendor incident notice expectations	Major ICT incident reporting	Incident and resilience reporting
Concentration	Considered in planning	Preliminary concentration assessment	Concentration and CTP awareness
Exit and termination	Termination planning	Documented exit strategies	Stressed exit plans
Reporting	Board and management reporting	Register submission to authorities	Notification of material outsourcing

LIFECYCLE EXPECTATIONS (INDIA, SINGAPORE AND PHILIPPINES, AUSTRALIA AND NZ)

Stage	India (RBI, SEBI)	Singapore and Philippines	Australia and NZ
Governance and policy	Board-approved outsourcing policy	Board oversight of material outsourcing	Service provider management policy
Inventory and register	Inventory of IT outsourcing	Outsourcing register	Register of material arrangements
Planning and risk assessment	Materiality assessment	Materiality and risk assessment	Link to critical operations
Due diligence	Documented due diligence	Due diligence before commitment	Due diligence scaled to materiality
Contracting	Audit and access for RBI	Access for the supervisor	Required terms for material arrangements
Ongoing monitoring	Periodic review of providers	Ongoing monitoring and audit	Monitoring, control testing (CPS 234)
Incidents	Incident reporting duties	Incident notification to MAS or BSP	Notification of material incidents
Concentration	Concentration risk	Concentration considered	Fourth-party and concentration view
Exit and termination	BCP and exit plans	Exit and continuity plans	Exit and continuity within tolerance
Reporting	Board and regulator reporting	Supervisory reporting	Annual register submission to APRA

LIFECYCLE EXPECTATIONS (MIDDLE EAST AND CROSS-SECTOR OVERLAYS)

Stage	Middle East (SAMA, CBUAE)	Data protection (GDPR, DPDP, PDPL)	Sector (HIPAA, PCI DSS, NYDFS)
Governance and policy	Board-approved outsourcing policy	Accountability of controller	Written TPSP security policy

Stage	Middle East (SAMA, CBUAE)	Data protection (GDPR, DPDP, PDPL)	Sector (HIPAA, PCI DSS, NYDFS)
Inventory and register	Register of outsourcing	Record of processors	List of TPSPs and BAs
Planning and risk assessment	Materiality assessment	Assessment of processing risk	Risk-based classification
Due diligence	Due diligence, cyber review	Sufficient guarantees from processor	Due diligence before engagement
Contracting	Regulator access, data location	Processor contract, flow-down	BAA, written TPSP agreements
Ongoing monitoring	Periodic assessment	Audits and inspections	Annual compliance status check
Incidents	Incident notification	Breach notification chain	Breach and cyber event notice
Concentration	Offshore and concentration review	Transfer and sub-processor mapping	Not a primary focus
Exit and termination	Exit plans	Return or deletion of data	Return or destruction of PHI and data
Reporting	Approval or notification	Records available to authority	Certification or attestation where required

Where regimes diverge

Five areas account for most of the local work. Plan annexes around them rather than around countries.

Register formats

DORA prescribes a structured register of information with defined templates and identifiers. APRA expects a register of material arrangements submitted on its schedule. PRA, RBI, MAS and EBA registers each have their own expected fields. The workable pattern is one master inventory with a superset of fields, from which each local register is exported. Maintain field-level mapping tables and reconcile each export to the master before submission.

Notification to regulators

Timing and triggers differ: before entering material outsourcing, within a set period after entering or changing a material arrangement, before offshoring, or on designated events. Some Middle East regimes expect engagement or approval before material or offshore arrangements. Build a notification matrix by entity and trigger, with an owner and a clock.

Data localization and transfer

Payment data localization in India, conditions on outsourcing outside Saudi Arabia, EU and UK transfer rules, and national privacy laws can restrict where data is stored or processed. Capture data location per service (primary, backup, support access) in the vendor record, not in a contract footnote.

Audit and access rights for regulators

Most regimes require that the supervisor, not just the firm, can access information, premises and records of the provider for material arrangements. Pooled audits and certifications can support this but rarely replace it. Keep a clause library with local variants and track which contracts contain which variant.

Board approval and accountability

Some regimes require board approval of the policy only; others expect board or senior management approval of specific material arrangements, or a named accountable executive. Document the approval path per entity and keep minutes as evidence.

HYPOTHETICAL EXAMPLE: ONE VENDOR, FOUR LABELS

A hypothetical group uses a single cloud-based core processing provider for its US bank, EU payments institution, UK branch and Australian subsidiary. Internally the vendor is tiered Critical. The vendor record shows: critical activity (US), ICT third-party service supporting a critical or important function (EU), material outsourcing supporting two important business services (UK), and material service provider for a critical operation (Australia). One due diligence file and one SOC 2 Type II review serve all four; local annexes add the DORA register entry, the PRA notification, and the APRA register row and offshoring notification.

Building one control set

A single control set should be written as control objectives with defined evidence, then tagged with the regimes each satisfies. That makes testing and examiner mapping mechanical rather than interpretive.

CORE CONTROL OBJECTIVES AND EVIDENCE

Control objective	Evidence	Regimes satisfied
A board-approved TPRM policy defines scope, roles and risk appetite	Policy, approval minutes, review log	All

Control objective	Evidence	Regimes satisfied
A complete vendor inventory exists with tier and local labels	Inventory extract, reconciliation to AP and contracts	All; DORA, APRA, PRA registers
Each engagement is risk-assessed and tiered before contract	Intake record, inherent risk rating, tier rationale	All
Due diligence depth follows tier	Due diligence file, SOC report review, questionnaire	All
Contracts include required clauses	Clause checklist, executed contract	DORA, PRA, RBI, MAS, APRA, HIPAA, GDPR
Critical vendors are monitored on a set cadence	Monitoring log, reassessment, KPI and SLA reports	All
Vendor incidents are notified, triaged and escalated	Incident register, notification records	All; DORA, NYDFS, HIPAA, APRA
Concentration and fourth parties are assessed	Concentration analysis, fourth-party map	DORA, OSFI, RBI, APRA, US
Exit plans exist and are tested for critical vendors	Exit plan, test results, data return certificates	DORA, EBA, PRA, RBI, MAS, APRA
Findings are remediated or formally accepted	Findings log, risk acceptance with approver	All
The board receives regular TPRM reporting	Board packs, minutes	All

Testing approach

Internal audit and second-line testing should cover design and operating effectiveness. For design, walk through one vendor per tier from intake to approval: inspect the intake record, confirm the tier rule was applied, confirm the due diligence steps match the tier, and trace the approval to someone with authority under the policy. For operating effectiveness, sample from the inventory, not from the population the first line offers. A common approach is to sample more heavily from critical and material vendors, include vendors onboarded in each jurisdiction, and include at least some terminated vendors to test exit evidence.

Test the local annexes separately. Reconcile each regulatory register export to the master inventory, check that notification clocks were met for new material arrangements in the period, and confirm contract clause variants match the entity.

WHAT EXAMINERS AND AUDITORS ASK

- Show the inventory and how it reconciles to accounts payable and the contract repository.
- Explain how criticality is determined and how it maps to our local definition.
- Walk through the due diligence file for this critical vendor, including SOC report review and CUECs.
- Show the contract clauses for audit, access, sub-contracting and termination.
- Show the exit plan and evidence it was tested or reviewed.
- Show the last board report and how issues were escalated.

Standards as the common technical baseline

Regulatory instruments tell you what outcomes to achieve; technical standards give a shared language for the security and resilience controls you assess at the vendor. Using them as the baseline lets one assessment serve many regimes.

- NIST CSF 2.0 (February 2024) adds a Govern function, including the GV.SC Cybersecurity Supply Chain Risk Management category, which covers strategy, supplier prioritization, requirements in contracts, due diligence, monitoring, and post-relationship activities.
- NIST SP 800-161r1 provides detailed cybersecurity supply chain risk management practices, useful for technology and software vendors and for reaching into sub-tier suppliers.
- ISO/IEC 27001:2022 Annex A controls 5.19 to 5.23 cover supplier relationship security, addressing security in supplier agreements, the ICT supply chain, monitoring and change management of supplier services, and use of cloud services.
- ISO/IEC 27036 gives lifecycle guidance for information security in supplier relationships.
- SOC 2 reports (Trust Services Criteria) and SOC 1 reports (internal control over financial reporting) are the most widely available independent assurance. Review Type II over Type I, read exceptions and opinion modifications, identify carved-out subservice organizations, map CUECs to your own controls, and obtain bridge letters for gaps.

Map each questionnaire question and each control domain to these standards once. When a regulator asks how you assess a vendor's access control or incident response, you point to the same control, the same evidence and the same standard reference in every jurisdiction.

Operating model and keeping the map current

A global policy with local annexes

The model that scales is a single global TPRM policy and standard, owned by the group TPRM function, with short local annexes owned by each legal entity. The global documents define lifecycle, tiers, control objectives, evidence and roles. Each annex states only what is different: local terminology mapping, register format, notification triggers and timelines, data location rules, contract clause variants, approval authorities, and local reporting.

- Group TPRM owns the method, inventory, tier scale and shared vendor assessments.
- Local risk and compliance own annexes, local registers and regulator relationships.
- Vendor owners in the business own the relationship, performance and first-line monitoring.
- Internal audit tests the global control set and each annex on a risk-based rotation.

Maintaining the map as rules change

Treat the regulatory map as a controlled document. Assign an owner, keep a version history and review it at least annually and whenever a relevant instrument is issued, amended or reinterpreted. Horizon scanning should cover consultation papers and implementing standards, not only final rules, because register templates and notification formats often change in technical standards. For each change, record the impact on the control set, the annex, the register fields and the training, then close the change with evidence.

KEEP CAVEATS VISIBLE

Several instruments in this paper have phased or evolving timetables, including DORA technical standards, SEBI CSCRF implementation, DPDP implementing rules and the UK CTP designations. Record the source and date you relied on for each map entry so reviewers can see when it needs a refresh.

Examiner requests and a readiness checklist

Examiners in different jurisdictions ask for similar things in different formats. A US examiner may request the inventory, board reports and a sample of due diligence files. An EU supervisor may start from the register of information. A PRA supervisor may focus on material outsourcing notifications and exit plans for important business services. APRA may test the register of material

arrangements against critical operations and tolerance levels. The efficient response is a standing package: the same underlying evidence, indexed to each regime's request list, with the local register export and annex attached.

- [ ] Global TPRM policy and standard approved by the board, reviewed within the last year
- [ ] Local annexes for each regulated entity, with owners and review dates
- [ ] One master vendor inventory with internal tier and local labels per vendor
- [ ] Field mapping from the master inventory to each regulatory register format
- [ ] Documented tier rules and rationale for every critical and material vendor
- [ ] Due diligence files matching tier depth, including SOC report reviews and CUEC mapping
- [ ] Contract clause library with local variants and a tracker of which contracts contain them
- [ ] Notification matrix by entity, trigger and deadline, with evidence of notifications made
- [ ] Data location recorded per service, including backup and support access
- [ ] Concentration and fourth-party analysis refreshed at least annually
- [ ] Exit plans for critical vendors, reviewed or tested, with data return evidence on termination
- [ ] Findings log with remediation owners, dates and formal risk acceptances
- [ ] Board and committee reporting pack with trends and escalations
- [ ] Internal audit coverage of the global control set and a rotation across annexes
- [ ] Regulatory map under change control with source dates

How VendRisk360 supports this

VendRisk360 is built so that one program can serve many regulators. Each vendor has a single record, with intake scoped by business case and data types, and criticality tiers (Critical, Material, Low risk) that drive assessment depth, sign-off and reassessment cadence, each configured to the organization's own policy. Because the tier scale is defined once, the mapping to local definitions such as critical activity, critical or important function or material service provider is set once in policy and applies consistently to every vendor record.

Assessments are a point-in-time, inside-out review across 30+ control domains, based on the artifacts vendors provide. Your analysts perform them, or VendRisk360 assessors do through Comprehensive Vendor Risk Assessment Services, and a named reviewer signs off with the decision recorded in the audit trail. SOC 1 and SOC 2 review covers exceptions, carve-outs, subservice organizations and CUECs, so one review can be reused across entities. Findings flow into remediation plans or formal risk acceptance, and multi-stage sign-off enforces segregation of duties with a sign-off certificate.

Between assessments, continuous monitoring adds the outside-in view: the vendor's external attack surface, shadow infrastructure, indicators of compromise, breaches and security incidents, adverse news and litigation, regulatory and enforcement actions and sanctions, routing confirmed-only alerts to the vendor owner. Nth-party intelligence maps fourth-party and nth-party relationships across vendors to show concentration, systemic risk and blast radius. Offboarding captures exit evidence such as access revocation and data return or destruction certificates.

For regulators, Excel exports of registers and findings provide the data behind each local register, and the examiner package export bundles assessments, evidence, sign-offs and the audit trail. Nine board and executive decks, including the Regulator / Examiner Meeting and Concentration Risk Briefing decks, are available in PDF and editable PowerPoint and can be scheduled. The platform supports SSO (SAML/OIDC), mandatory MFA, row-level-security tenant isolation, encryption in transit and at rest, custom roles and a full audit trail.

How to work with VendRisk360. On the Vendor Lifecycle Management Platform, your team manages vendors, sends due diligence and evidence requests through the vendor portal, performs the review, records it and signs off, with every step tracked in a full audit trail. With Comprehensive Vendor Risk Assessment Services, you onboard the vendor and VendRisk360's certified assessors collect the evidence and follow up with the vendor, perform the risk assessment scaled to the vendor's tier with a second-expert quality review, and follow findings through remediation. You see each vendor's progress on the platform in near real time and keep final approval, as regulators expect. Continuous Monitoring Services add the outside-in view between assessments, and Report-Specific Reviews (SOC Report Review, Information Security Program Review and Business Continuity Program Review) are available standalone or alongside either. Assessors hold certifications such as CISSP, CISA, CISM, CRISC and ISO/IEC 27001 Lead Auditor and Lead Implementer, with PCI DSS implementation experience. AI is optional: where a customer opts in, it assists only with completeness checks and key-date extraction on vendor evidence and with an AI-assisted first pass on SOC reports that the expert assessor verifies. Every review, rating and sign-off is performed by an expert assessor or by the customer's own reviewers.

See how the platform lines up with each instrument on the regulatory coverage page, or book a demo to walk through a multi-jurisdiction setup.

About VendRisk360

VendRisk360 is an independent company providing a third-party risk management platform and expert services for regulated organizations: banks, credit unions, fintech and payments, healthcare and SaaS. The platform runs vendor lifecycle management, risk-tiered assessments, continuous monitoring, nth-party intelligence and board-ready reporting from one governed record per vendor, combining point-in-time, evidence-based review with continuous outside-in monitoring. Customers run it themselves on the Vendor Lifecycle Management Platform, or add Comprehensive Vendor Risk Assessment Services, Continuous Monitoring Services and Report-Specific Reviews delivered by certified VendRisk360 assessors.

Learn more at **vendrisk360.com** or write to **info@vendrisk360.com**.

This paper is general guidance for practitioners, not legal advice. Regulatory requirements change and vary by jurisdiction and institution; confirm your obligations with counsel and your supervisors.