EDITION · 2026

The OSINT vendor review checklist.

Twelve external signals every third party risk program should monitor between assessment cycles.

Key points

13	3	5	12
External signals	Vendor tiers	Playbook steps	Languages monitored

See risk before it's news.

HOW TO USE THIS CHECKLIST

A continuous OSINT layer for vendor risk programs

Vendor questionnaires answer what your suppliers say about themselves, on a cycle measured in months. This checklist covers what the rest of the world publishes about them between cycles — the external signal layer that closes the blind spot in standard third party risk programs.

It complements, not replaces, the TPRM platform you already operate. The signal taxonomy feeds escalation triggers into existing workflows in OneTrust, Prevalent, Black Kite, ProcessUnity, Aravo and equivalent systems of record.

RECOMMENDED MONITORING FREQUENCY BY VENDOR TIER

TIER	VENDOR PROFILE	OSINT REFRESH
Tier 1	Critical — operational, financial or regulatory dependency	Daily, with real time alerts on Tier-A signals
Tier 2	Important — material spend or data exposure, replaceable	Weekly, with alerts on Tier-A signals
Tier 3	Standard — low spend or low data third parties	Monthly, alerts on sanctions or material litigation only

Tier-A signal

Tier-A signals require immediate escalation regardless of vendor tier, typically sanctions additions, material regulatory enforcement and confirmed cybersecurity incidents involving customer data. Tier-B signals (sentiment shifts, executive turnover) are reviewed in cycle. Tier-C signals (single source litigation, ESG controversies) are aggregated weekly.

FINANCIAL DISTRESS SIGNALS

Financial distress signals

01

Credit rating actions

Independent credit quality assessment by S&P, Moody's, Fitch or DBRS — downgrades, negative outlooks, watch list placements. Often the earliest formal validation that institutional creditors share the market's concerns.

WHERE TO DETECT

Rating agency announcements; financial press; SEC 8-K filings; bond spread movements.

ESCALATION TRIGGER

Any downgrade across investment-grade boundaries (BBB to BB) or two notch action in a single review.

02

Senior executive departures

Unscheduled departure of CFO, CEO, COO, board chair or audit committee chair. Especially significant without a named successor or coincident with quiet quarters.

WHERE TO DETECT

Corporate press releases; 8-K Item 5.02; LinkedIn; proxy statements; trade press.

ESCALATION TRIGGER

CFO departure with no succession plan; CEO plus audit chair within 6 months.

03

Distressed financing press

Public reporting of covenant breach, restructuring advisor engagement (Houlihan Lokey, Alvarez & Marsal, FTI), bridge loans, DIP financing discussions, or going concern disclosure language.

WHERE TO DETECT

Bloomberg, Reuters, WSJ, FT; audited filings; debtinvestor services; advisor mandates.

ESCALATION TRIGGER

Any restructuring advisor retained; covenant waiver request; going concern qualification.

OPERATIONAL DISRUPTION SIGNALS

Operational disruption signals

04

Payment delays in vendor networks

Mentions of delayed or unreliable payments by the vendor, surfacing in its own suppliers' or customers' communications often the earliest evidence of working capital stress.

WHERE TO DETECT

Tradepress complaints; supplier earnings call mentions; specialty publications.

ESCALATION TRIGGER

Three or more independent supplier mentions of payment delay in a quarter.

05 Facility incidents

Fire, explosion, accident, weather event, or force majeure affecting a vendor production, storage or service site including third tier facilities your vendor depends on.

WHERE TO DETECT

Local news in local languages; emergency services bulletins; satellite imagery; supplier disclosures.

ESCALATION TRIGGER

Any incident at a single source component facility or affecting more than 10% of capacity.

06 Labour actions

Strikes, walkouts, mass layoffs, union organisation drives, or worker safety actions affecting vendor production capacity. Especially significant in single region concentrations.

WHERE TO DETECT

Local language press; union announcements; NGO worker rights reports; ILO databases.

ESCALATION TRIGGER

Any strike or walkout at single source production; greater than 5% workforce reduction.

07 Cybersecurity incidents

Public breach disclosures, ransomware claims (including by attacker groups on leak sites), regulatory cybersecurity filings (SEC Item 1.05), or advisories naming the vendor.

WHERE TO DETECT

Vendor press releases; SEC 8-K filings; threat intelligence feeds; ransomware leak sites; regulator notices.

ESCALATION TRIGGER

Any confirmed breach involving customer data, or ransomware claim with named victim disclosure.

08 Quality and recalls

Product safety recalls, voluntary withdrawals, regulator-mandated corrective actions, or material quality failures affecting customer-facing output.

WHERE TO DETECT

Regulator recall registries (FDA, NHTSA, EMA, CPSC, RAPEX); vendor press releases; specialty trade publications; class-action filings.

ESCALATION TRIGGER

Any Class I or urgent recall; multiple recalls within 12 months; recall affecting a product line sourced by your organisation.

REGULATORY AND SANCTIONS SIGNALS

Regulatory and sanctions signals

09

Regulatory investigations

Formal investigation or enforcement by competition, financial, environmental or sectoral regulators — DOJ, SEC, FTC, DG COMP, FCA, BaFin, FINMA, CFPB, OFAC and equivalents.

WHERE TO DETECT

Regulator press releases; vendor 8-K filings; legal press services; specialty publications.

ESCALATION TRIGGER

Any opened investigation by primary regulator; consent decree or settlement above materiality.

10

Sanctions list additions

Inclusion of the vendor entity, parent, beneficial owners or named executives on OFAC SDN, EU Consolidated, UK HM Treasury or UN sanctions lists. Includes PEP list additions.

WHERE TO DETECT

Sanctions lists refreshed directly from issuers; OSINT beneficial ownership cross reference; PEP databases.

ESCALATION TRIGGER

Any addition. This is always a Tier A signal regardless of vendor tier.

11

Material litigation

Filed or judged litigation that meets a materiality threshold like class actions, regulatory penalties, IP injunctions, or product liability judgments exceeding 1% of revenue.

WHERE TO DETECT

Court filing services (PACER, RECAP, equivalents); legal press; vendor disclosures; specialty trackers.

ESCALATION TRIGGER

Class action certification; adverse judgment exceeding materiality; injunction halting product line.

REPUTATION AND ESG SIGNALS

Reputation and ESG signals

12

Sustained sentiment shifts

A material and sustained downward trend in tone of coverage about the vendor — measured across hundreds of thousands of sources, multilingual, with topic level granularity. A single negative article is noise; a 60 day directional shift is signal.

WHERE TO DETECT

Media sentiment indices across global press; analyst note tone tracking; specialty coverage.

ESCALATION TRIGGER

Sustained negative sentiment exceeding 2 standard deviations from 12 month baseline for 30 plus days.

13

ESG controversies

Reported human rights, environmental or governance controversies — supply chain labour violations, environmental incidents, anti corruption press, governance failures. Increasingly relevant under CSDDD and CSRD.

WHERE TO DETECT

NGO reports; investigative journalism; ESG rating agency notices; regulator advisories; specialty trackers.

ESCALATION TRIGGER

Named in NGO investigative report; downgrade by primary ESG rating provider; regulator advisory.

INTEGRATION PLAYBOOK

From signal to escalation, inside your existing workflow

OSINT based monitoring is most useful when its output is wired into the systems your vendor risk team already operates. The five steps below are the same regardless of which TPRM platform you run.

01 **Tier your vendor portfolio against the signal framework**
Map each vendor to a tier based on operational dependency, data exposure and concentration risk. Decide which signals are Tier-A (immediate), Tier-B (cycle review), Tier-C (aggregated).

02 **Establish escalation thresholds before you start**
Decide what triggers a review—specific signal types, severity, recurrence. Document these before the first alert fires; thresholds set mid incident tend to be miscalibrated.

03 **Route signals into the existing system of record**
Configure the OSINT layer to open tasks, attach evidence and flag risk fields in your TPRM platform directly. Avoid a parallel risk register the vendor team has to check separately.

04 **Run quarterly threshold review**
Calibrate thresholds against false positive rate and missed signal rate. Most programs start too sensitive (alert fatigue) and ease them over 2 to 3 quarters.

05 **Document for audit**
Regulators increasingly expect evidence that third party risk programs cover the period between scheduled assessments. The signal log is that evidence.

ABOUT THIS CHECKLIST

From manual scanning to automated signal

13 signal framework in this checklist is documentable, defensible and operable by a vendor risk team using manual analyst time up to a point. That point is usually around fifty critical vendors. Beyond that scale, the multilingual press, regulatory, sanctions, court filing and ESG data surface area exceeds what manual scanning can keep up with in real time.

svChain is the automated layer that runs this framework continuously against a customer's vendor portfolio. It monitors tens of millions of companies across hundreds of thousands of sources in 12 languages, classifies events against the twelve signal taxonomy and feeds escalation triggers into your existing TPRM workflow.

ABOUT SEMANTIC VISIONS

Semantic Visions is a Prague based AI powered OSINT and risk intelligence platform. We monitor tens of millions of companies across hundreds of thousands of sources in 12 languages to surface third party, supply chain and reputational risk before it appears in self reported channels.