ComplyScore®

Solution Brief

Continuous Monitoring That Triggers Action

Moving from scheduled reviews to real-time signals that already know what to do next

The Challenge

Annual assessments produce a risk score. Continuous monitoring produces an early warning. Most programs have only one of those. A vendor that passed its assessment in January can sustain a financial decline, disclose a breach, or lose a critical certification before the next scheduled review catches it.

The gap between assessment cycles is where incidents develop. Organizations that found out about a critical supplier's breach through the news were not unlucky; they had no mechanism that could have caught it sooner.

Where Programs Get Stuck

No signal between cycles

Assessment scores age from the moment they are generated. Vendor risk changes continuously, but scheduled reviews only look once a year.

Alerts buried in inboxes

Monitoring tools generate signals that arrive via email, get triaged manually, and regularly age without any follow-up or documented closure.

Historical data, not live intel

D&B and S&P subscriptions show what happened last quarter. Organizations need to know what is happening to a vendor right now.

What ComplyScore® Changes

ComplyScore® monitors vendor risk continuously across cyber breach disclosures, financial distress signals, sanctions watchlist changes, adverse media, and regulatory enforcement actions. Alerts are structured actions, each categorized by severity, routed to the right risk owner, and linked to a pre-staged remediation task.

Without ComplyScore®	With ComplyScore®
Material vendor risk events discovered weeks after occurrence	Risk events surfaced within hours via continuous signal aggregation across global and regional feeds
Monitoring alerts sent via email; follow-up tracked in spreadsheets	Alerts routed directly to named risk owners with pre-staged remediation tasks and escalation paths
Same monitoring cadence for all vendor tiers regardless of exposure	Configurable monitoring portfolios: high-risk vendors monitored continuously, lower tiers on automated schedules
No connection between monitoring alert and assessment cycle	Threshold breach triggers a formal reassessment automatically; delta comparison to prior assessment included

Key Capabilities

Configurable risk signal portfolios

Teams define what to monitor per vendor tier: cyber signals, financial distress, sanctions, adverse media, regulatory actions, and ESG flags.

Score-threshold alerting

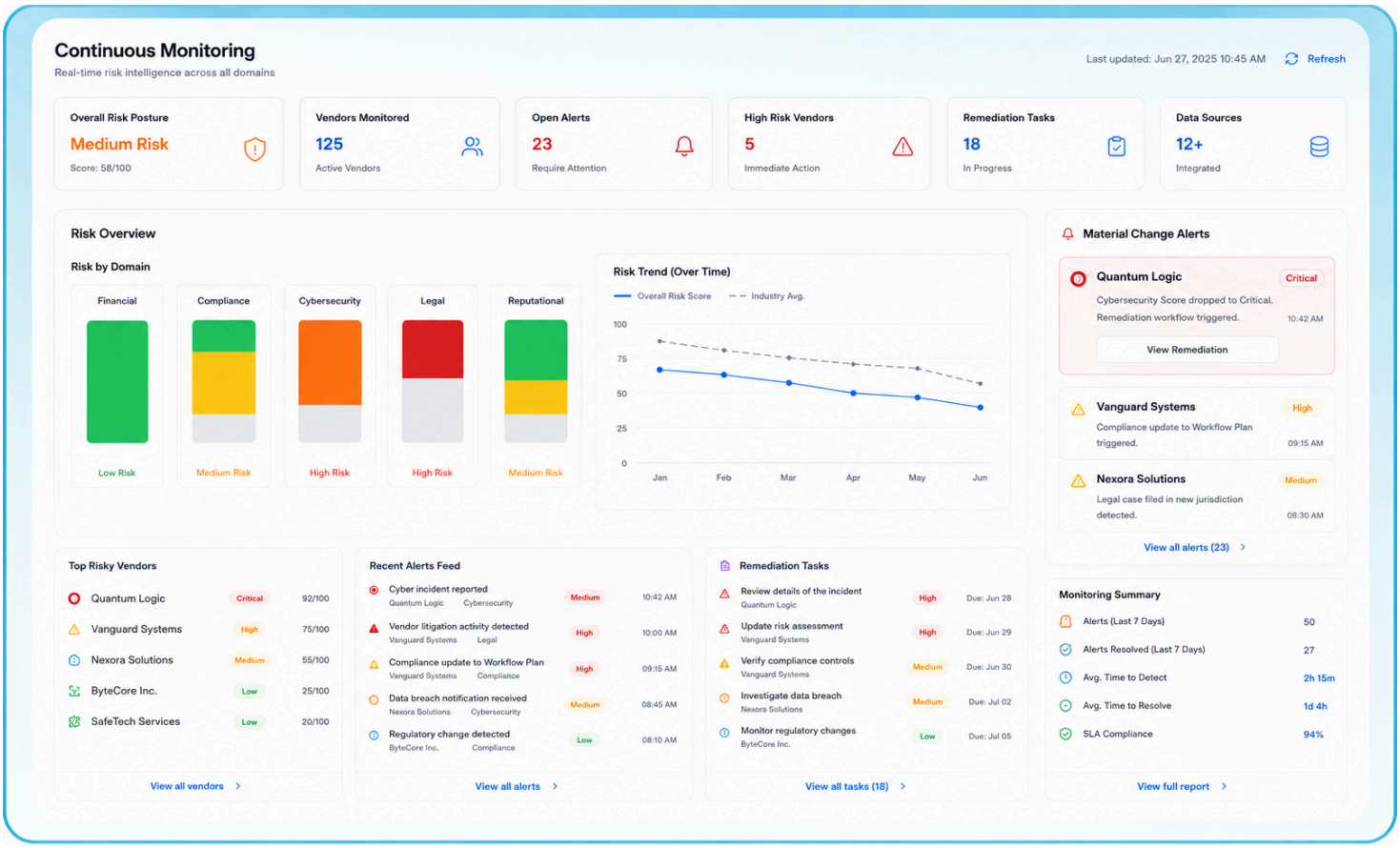
When a vendor's real-time risk score drops below a defined threshold, a priority alert is routed automatically to the relevant risk owner.

Actionable alert routing

Alerts are categorized by severity (information, remediation-required, escalation-needed) and linked to pre-staged response tasks.

Reassessment triggers

A material monitoring signal can automatically initiate a formal control assessment, with the prior assessment linked for delta comparison.



60%

Reduction in manual monitoring effort

Hours

To surface material risk events

vs. weeks under manual monitoring

90-95%

Vendor portfolio coverage

ATLAS SYSTEMS | ComplyScore®

Learn how real-time monitoring replaces your annual review cycle

Get A Demo

sales@atlassystems.com atlassystems.com/complyscore