

From Diligence To Live Controls

Sentora's front-to-back risk
infrastructure for vault curation

VAULT DETAILS & RISK REPORTS



Vault curation requires more than just an onboarding review because risk profiles evolve significantly after deployment. Protocol parameters can shift after approval, while collateral composition can vary across markets and oracle routes may change during operations. Furthermore, liquidity can exit faster than standard review cycles can address, and security events can impact exposure before a formal committee meeting can be convened.

Sentora addresses this problem through structured infrastructure. The process begins with a DDQ review of blockchains, protocols, and assets, followed by the establishment of risk framework policies for Sentora-Vaults, Smart Yield clients, and Protocol-Vaults. These policies are then codified into enforceable mandates, protocol configurations, risk triggers, and monitoring systems, which drive alerts, reporting, and escalation.

In this front-to-back operating model, the DDQ process defines the approved universe while the risk framework establishes acceptable exposure. The Sentora Risk Application then translates both into live controls, with reporting and escalation closing the loop through a governed review.

1. The Problem: Vault Risk Is Continuous

Vault curation is a continuous control process. It spans blockchain infrastructure, protocols, assets, liquidity, oracles, governance, and operating process.

A vault can be sound at onboarding and still change its risk profile after deployment. Protocol parameter control depends on the venue design.

In Aave and Kamino, core parameters such as supply caps, borrow caps, liquidation settings, oracle routes, and market configuration are controlled by the protocol or its governance process. Sentora must monitor these settings, assess proposed changes, and engage with the protocol where adjustments are required.

In Euler and Morpho, curators have direct control over many of these parameters and must govern them through disciplined internal policy. Assets may also evolve through privileged roles, bridge dependencies, redemption mechanics, or shifting counterparty exposure, just as liquidity often migrates fluidly across venues and chains. Furthermore, security conditions can transform rapidly, often outside the cadence of a scheduled review.

This dynamic environment creates a clear operational requirement for institutional DeFi capital: the approved universe must stay current, framework limits must remain enforceable during operation, and monitoring needs to be live throughout deployment. Consequently, escalation protocols must be clearly defined well before any exposure risks becoming disorderly.

This structured approach is rapidly becoming the standard for institutional vault curation, where assets must be rigorously classified prior to onboarding. A comprehensive technical review is essential, spanning token behavior, oracle design, privileged access, and bridge risks, while also accounting for audit history and operational dependencies. These reviews connect directly to

parameter decisions and exposure limits, establishing a clear path for monitoring, remediation, and periodic reassessment.

Sentora operationalizes this through an integrated infrastructure: the DDQ workflow builds the primary evidence base, while the risk framework defines the boundaries of acceptable exposure. The Sentora Risk Application then translates these policies into live controls, alerts, and reports, ensuring that every facet of the curation process remains subject to governed review.

The outcome is a governed infrastructure layer for disciplined capital deployment. Sentora treats vault risk policy as an operating control system with clear ownership across diligence, policy, monitoring, reporting, and governance.

2. Sentora's Front-To-Back Risk Architecture

Sentora's risk architecture begins before capital deployment, anchored by a structured DDQ process for blockchains, protocols, and assets. Each review establishes a comprehensive evidence base that supports ongoing diligence, including inquiries, decision-making, and recurring review cycles.

The next layer is policy. Sentora-Vaults carry the highest policy importance because the organization operates within the client mandate and controls deployment across approved strategies. Smart Yield clients sit within this Sentora-Vault policy layer because strategy activity, on-chain controls, and client mandates remain linked. Protocol-Vaults carry a narrower but still governed role. Sentora acts as curator through liquidity allocation, parameter review, asset coverage, and ongoing monitoring.

The third layer is translation. Approved blockchains, protocols, and assets become operating controls, including allowlists, blocklists, client restrictions, protocol vault directory entries, LLTV settings, maximum borrow caps, risk trigger thresholds, collateral tiers, cap utilization thresholds, oracle deviation thresholds, and security watchlists.

The fourth layer is live monitoring. The Sentora Risk Application checks exposure, collateral composition, protocol parameters, security events, data freshness, and report output. These surfaces operate across scheduled jobs, live dashboards, alerting routes, and API integrations. For Smart Yield clients, engineering on-chain bots execute on-chain controls and trigger actions. The Risk Application remains the policy, configuration, evidence, and reporting layer that connects those bot controls back to the governed framework.

Finally, the governance layer closes the loop by moving alerts into a structured process of acknowledgement, escalation, and review. This framework is overseen by the Risk Committee, ensuring that any changes to exposure, capital deployment, or controls follow a governed and disciplined path.

The architecture can be summarized in one operating chain.

This chain is the central statement of the report. Sentora connects diligence, policy, controls, monitoring, alerts, reporting, and escalation into one disciplined infrastructure layer.

Figure 1: Sentora front-to-back operating chain

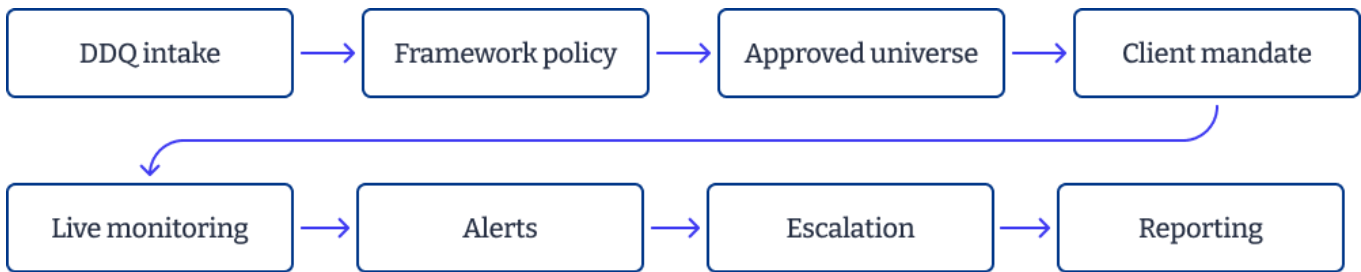
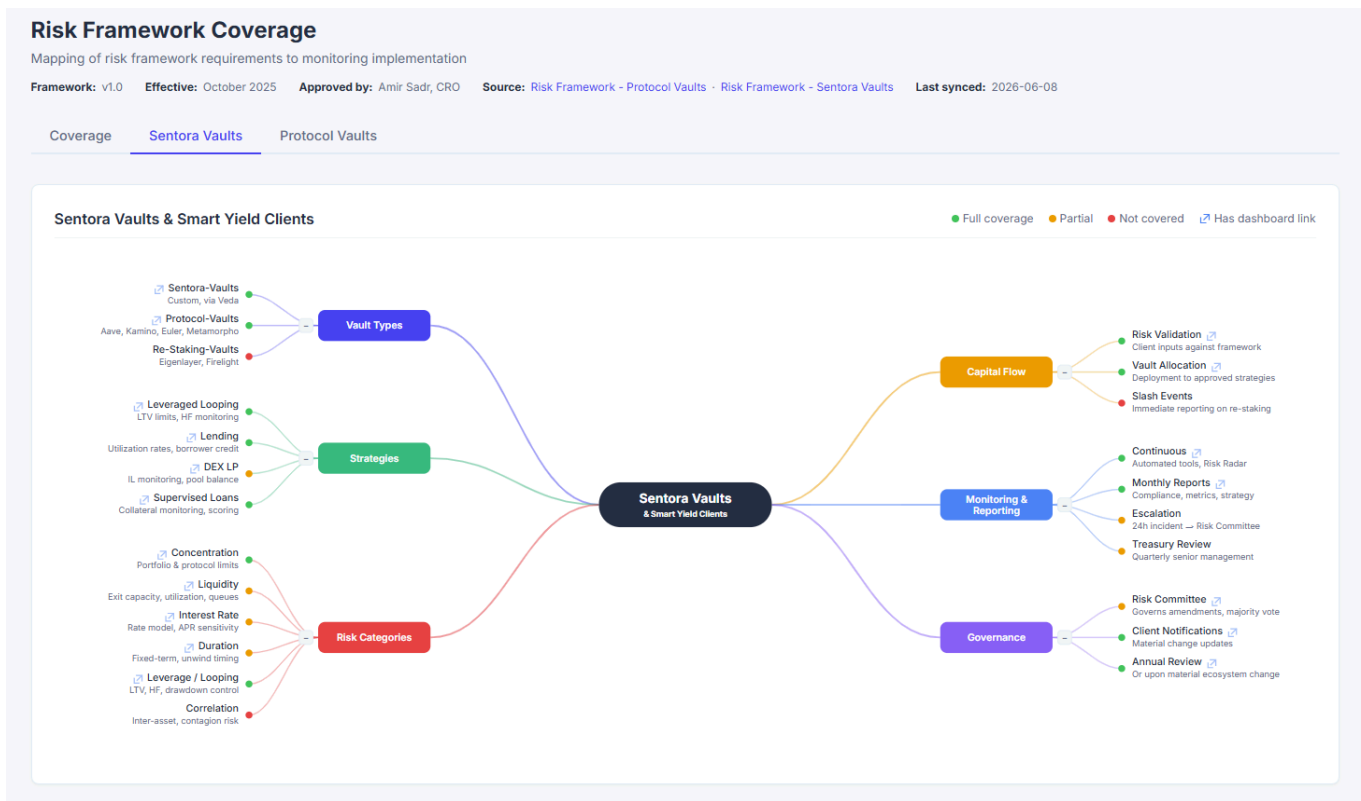
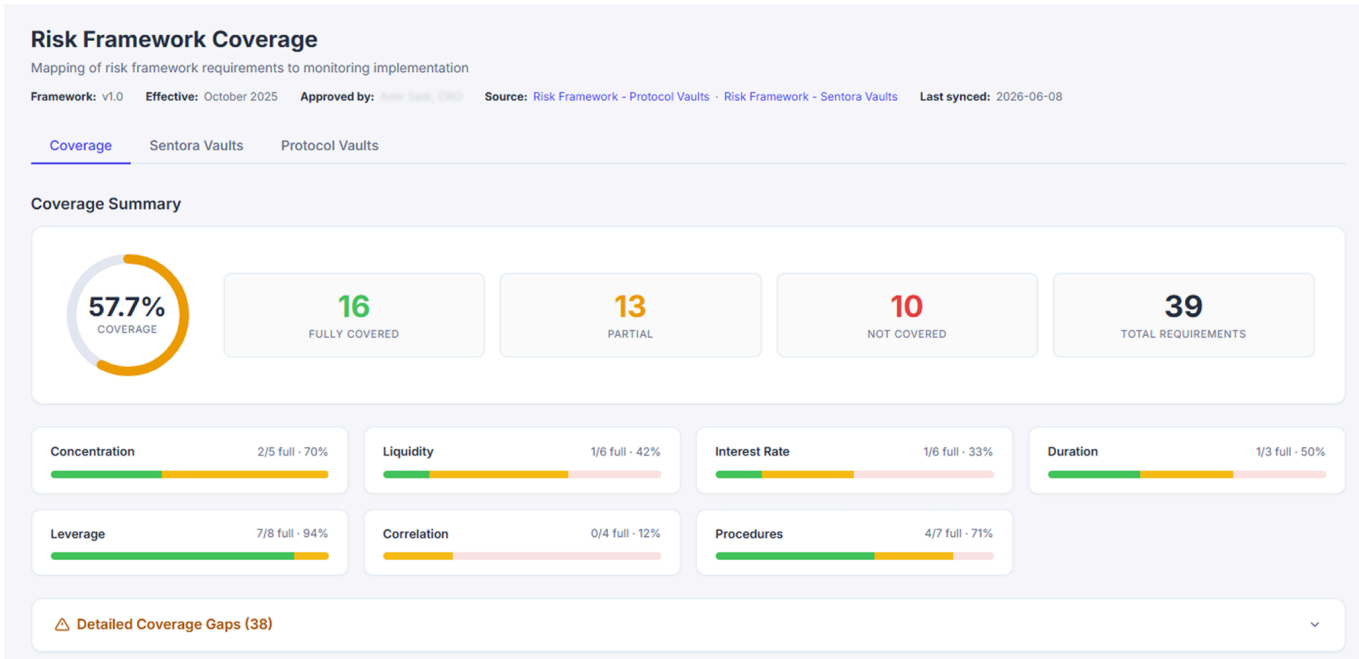


Figure 2: Risk framework policy architecture





The Sentora-Vault framework view shows why policy is central to the operating model. It integrates vault types, Smart Yield clients, and approved strategies with capital flow, monitoring, reporting, and governance. Furthermore, the framework effectively distinguishes between full, partial, and uncovered coverage areas, providing the visible control surface essential for true risk ownership.

The Sentora Risk Application has been operating in production since January 2026. The production volume contains DDQ records, protocol vault configs, alert configuration, Smart Yield trigger tokens, and report archives. The process exists in the application, in the data model, in monitoring surfaces, and in reporting output.

The counts below are aggregate production signals.

Operating evidence

Evidence area	Proxy
DDQ dossiers	25
DDQ review cycles	40
DDQ evidence items	116
DDQ questions	671
Protocol vault configs	18
Risk alert modules	17

Evidence area	Proxy
Risk alert threshold keys	458
Smart Yield trigger tokens	3
Report files	21,931

3. DDQ Intake And Vetting

The front-to-back process starts with research intake. Before a blockchain, protocol, or asset can support deployment, Sentora's Research team prepares an initial protocol overview. This report establishes the first structured view of the candidate, covering protocol category, key metrics, capital flow, participant roles, market structure, current pools, smart contract architecture, audit history, technical risks, and an initial risk rating.

The Risk team then converts this research base into a formal DDQ dossier that records the protocol, token, chain, counterparty context, requested review scope, decision state, review timing, and commercial notes where relevant. This makes the first risk control point explicit: a candidate enters the risk process as a review object before it becomes part of the approved universe.

The DDQ workflow is evidence-driven. The Risk Application supports research reports, uploaded files, pasted notes, public web research, issuer responses, meeting notes, and structured question packs. Evidence can be uploaded as PDF, DOCX, XLSX, PPTX, HTML, TXT, Markdown, or CSV. The system extracts text where possible and stores the material inside the dossier, creating an auditable basis for review.

Each dossier can move through numbered review cycles, which can be opened for initial review, follow-up, material change, or re-review. Questions move through a status workflow from draft to open, sent, answered, follow-up required, closed, or NA. This gives the risk team a controlled record of what was asked, what was answered, what evidence supported the answer, and what decision followed.

AI-assisted question generation strengthens the diligence process while preserving risk ownership. The system uses dossier metadata, the Research team's protocol overview, uploaded evidence, existing question history, issuer responses, and DDQ-safe public research to generate targeted risk questions. Analysts review, refine, send, and close the questions. The tool increases coverage and consistency, while the decision remains governed by Sentora's risk process.

The decision field is the gate. A dossier can remain pending, move to research review, receive approval, receive conditional approval, be rejected, or be assigned to a later review cycle. This

decision state determines whether the blockchain, protocol, or asset can enter the approved universe. The next policy layer then determines how approved exposure can be used.

Production data shows that DDQ is an active operating process. The Railway production evidence snapshot contains 25 DDQ dossiers, 40 review cycles, 116 evidence items, 671 questions, and 447 question answers. These counts show that the DDQ process has an operating record across intake, evidence, questions, responses, and review cycles.

Figure 3: Risk DDQ intake and review workflow

Risk DDQ

Versioned due diligence dossiers for protocol and token assessments.

Create Dossier -

Create Dossier

Start a protocol/token review with all three Sentora modules available from day one.

Protocol

Token

Chain

Counterparty

Request Date

Requested By

Internal Slack Thread

Priority

Not set

Status

Active

Initial Decision

Pending DDQ

Next Review Date

Estimated Review Time

Risk-Deadline

What This Slice Does

The first implementation pass is focused on intake, structure, and evidence management.

- Create one dossier per protocol/token pair.
- Open a new review cycle automatically on creation.
- Capture pasted text and file uploads as evidence.
- Keep Sentora styling and navigation consistent with the existing app.

DDQ AI Model Policy

Standard analysis uses c1aude-sonnet-4-6. Hard cases can be escalated to c1aude-opus-4-6 without changing the rest of the app.

DDQ Evidence

DDQ area	Production signal
DDQ dossiers	25
DDQ review cycles	40
DDQ evidence items	116
DDQ questions	671
DDQ question answers	447

The DDQ stage converts external complexity into a governed internal record, defining the candidate universe before policy sets exposure limits, controls, monitoring, and escalation.

4. Policy Translation Into Controls

Policy has value when it becomes executable. Sentora translates research, DDQ decisions, and framework requirements into controls that can be configured, reviewed, monitored, and escalated.

The first control layer is the approved universe. DDQ determines which blockchains, protocols, and assets can support deployment. A review can remain pending, receive conditional approval, be rejected, or move into re-review. This decision state keeps review status tied to deployment eligibility.

The second control layer is research model design. Sentora's Research team designs analytical models and tools that support parameter setting, market review, and exposure analysis. LLTV and maximum borrow cap models are part of this layer. These models assess liquidation buffers, debt capacity, collateral behavior, liquidity depth, and market stress conditions. The broader research toolkit includes internal analysis and public infrastructure such as Risk Radar (<https://defirisk.sentora.com/>).

The third control layer is Risk team vetting. The Risk team reviews the model logic, assumptions, outputs, and operating use case before a model version becomes part of the production control framework. Once approved, the model output can inform protocol parameters, monitoring thresholds, and governance review. This creates a disciplined path from research design to risk approval to operational control.

The fourth control layer is venue-specific parameter authority. Protocol designs differ. In Aave and Kamino, core parameters such as supply caps, maximum borrow caps, liquidation settings, oracle routes, and market configuration are controlled by the protocol or its governance process. Sentora monitors these settings, assesses proposed changes, and engages with the protocol where adjustments are required. In Euler and Morpho, curators have direct control over many parameters. In these cases, Sentora governs those controls through internal policy, approved models, and production monitoring.

The fifth control layer is the client mandate. Client configuration converts the framework into allowed and blocked protocols, allowed and blocked strategies, blockchain limits, token restrictions, bridge restrictions, fee settings, LTV limits, leverage limits, exit maturity limits, and health factor thresholds. Repo defaults sit in ``vault-clients/clients/``. Runtime overrides sit in ``DATA_DIR/clients/``. The application reads the override first and falls back to the repo default, which creates a disciplined path from approved policy to active mandate.

The sixth control layer is protocol vault coverage. The Protocol Vault Directory defines which Morpho, Euler, and Kamino vaults the platform actively tracks. Production evidence shows 18 protocol vault configs across Euler, Kamino, and Morpho. These configs capture vault identity,

protocol, chain, status, eligible collateral, LTV, LLTV, supply caps, maximum borrow caps, oracle type, liquidity fields, and interest rate model fields.

LLTV and maximum borrow caps reside at the intersection of research, policy, and live risk control. Research designs and refines these models, with the Risk team vetting each material version before the production system implements the approved outputs into monitoring and governance workflows. Since market structure, protocol design, liquidity, and collateral behavior shift frequently, this remains a continuous process: Research updates the models, and Risk reviews each material update before any production implementation.

The seventh control layer is risk trigger configuration. Trigger files translate policy categories into threshold rules. The current protocol vault trigger configuration contains nine global thresholds, four health-score threshold groups, and eight oracle deviation thresholds. These thresholds cover rate movement, supply movement, borrow movement, distance to kink, loan aggressiveness, slippage, whale health score movement, health score floors, and oracle deviation limits.

Smart Yield controls sit inside this same policy translation model. The current trigger config includes health score and oracle deviation thresholds. Engineering on-chain bots execute the Smart Yield on-chain control logic outside the Risk Application. The Risk Application gives the risk team the governed visibility layer for these thresholds and connects the bot control model back to Sentora-Vault policy.

Figure 4: Protocol vault configuration controls

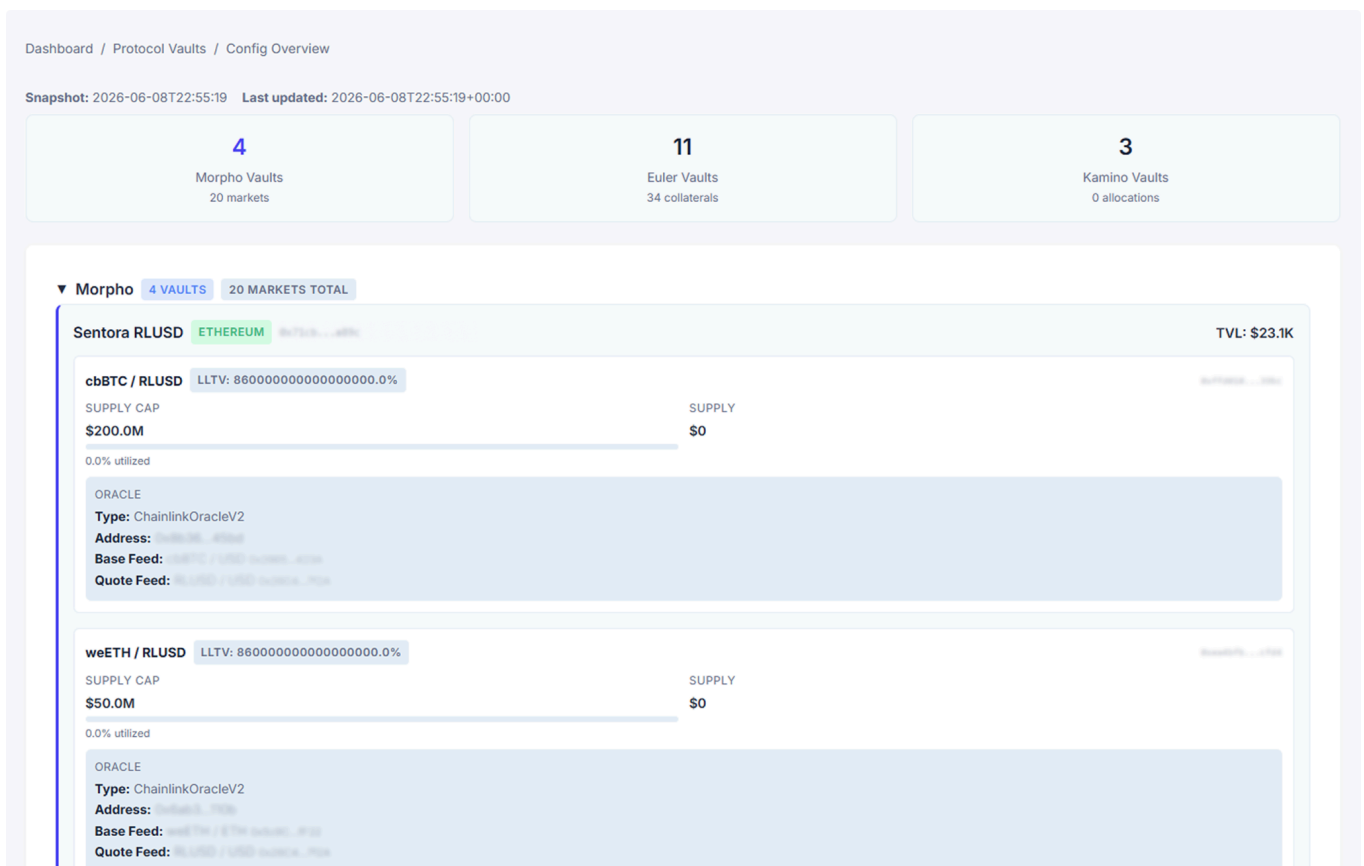


Figure 5: Risk trigger configuration controls

Protocol Vault Risk Triggers

Configure thresholds that trigger risk alerts for protocol vaults

Risk Trigger Configuration

These thresholds are used by the daily vault-check process to detect anomalous conditions across protocol vaults. Changes take effect on the next scheduled run. Global thresholds are entered as percentages (e.g., 5 = 5%). Vault list is loaded dynamically from [Protocol Vault Config](#) — add or remove vaults there and they appear here automatically.

Global Thresholds

Borrow Rate Daily Change

Triggers when borrow rate moves more than this

% > X%

Total Supply % Change

Triggers when total supply changes more than this

% > X%

Distance to Kink

Triggers when utilization is within this distance of the kink

% < X%

Slippage Threshold

Max acceptable slippage (negative = loss)

% < X%

Whale Health Score Change

Change in whale health score metric

% < X%

Supply Rate Daily Change

Triggers when supply rate moves more than this

% > X%

Total Borrows % Change

Triggers when total borrows changes more than this

% > X%

Loan Aggressiveness Weekly Change

Weekly change in loan aggressiveness ratio

% > X%

Slippage Max Deposit % Change

Change in max deposit slippage

% < X%

Control Evidence

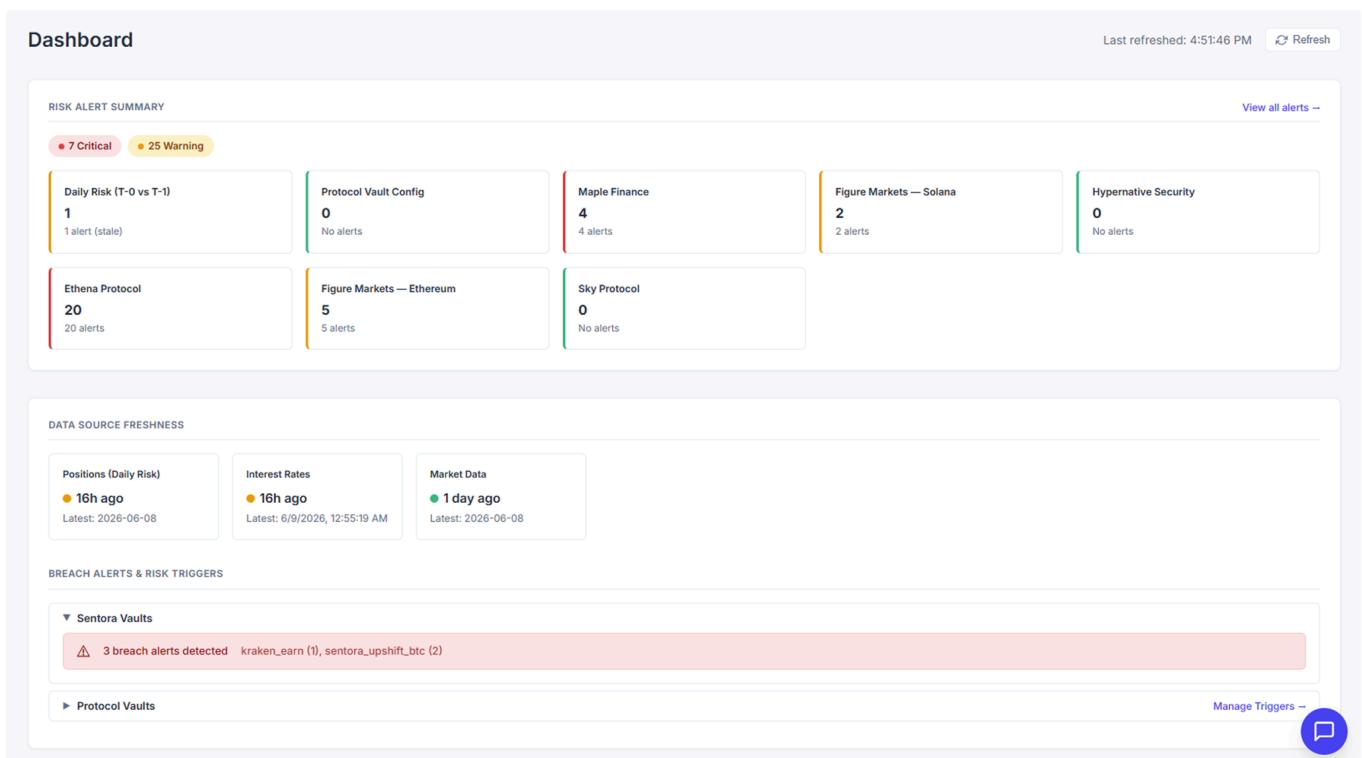
Control area	Operating signal
Production protocol vault configs	18
Euler protocol vault configs	11
Kamino protocol vault configs	3
Morpho protocol vault configs	4
Global protocol trigger thresholds	9
Health-score threshold groups	4
Oracle deviation thresholds	8

9

5. Live Monitoring And Alerting

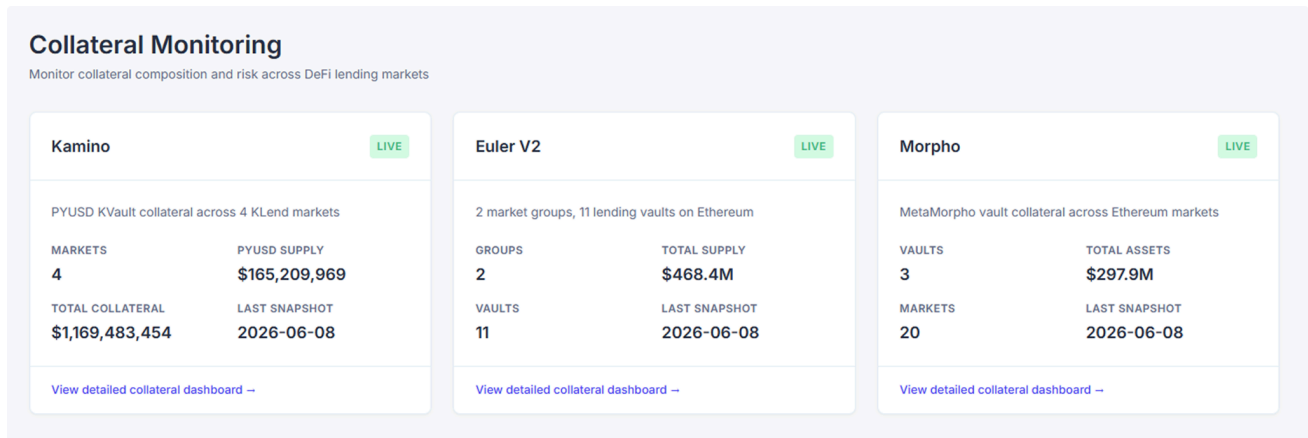
Controls must be tested against current data. Sentora uses the Risk Application to compare live and scheduled observations against the approved universe, client mandates, protocol parameters, trigger thresholds, and data quality expectations.

The first monitoring layer is scheduled execution. The daily-risk job runs at a specific time and produces position analysis, TVL checks, collateral snapshots, protocol data, and report outputs. The vault-check job runs on the same cadence and checks client restrictions and external vault dashboards. These jobs give the risk team a daily control point across capital deployment, exposure, and mandate compliance.



The second monitoring layer is collateral and parameter surveillance. The collateral monitoring dashboard covers Kamino, Morpho, and Euler, tracking collateral composition, risk tiers, historical snapshots, live refreshes, supply caps, maximum borrow caps, and cap utilization. The dashboard flags reserves near supply or borrow caps at 80 percent, 90 percent, and 100 percent utilization bands. This turns policy limits into visible risk states before liquidation or exit conditions become disorderly.

Figure 6: Collateral monitoring and cap utilization



The third monitoring layer is protocol configuration and rate movement. Protocol vault monitoring compares current parameters against prior baselines, highlighting changes in supply caps, maximum borrow caps, oracle fields, LLTV, collateral lists, market membership, liquidity, and allocation shifts. Risk triggers also monitor borrow rate movement, supply rate movement, total supply changes, total borrow changes, distance to kink, slippage, whale health scores, and oracle deviation. This is where configured controls become daily alert logic.

The protocol vault alert collector treats LLTV changes as critical alerts. It treats supply cap and borrow cap changes as warning alerts when the configured percentage threshold is exceeded. This makes core lending parameters part of the alerting surface and the metadata model. It also connects parameter governance to live risk operations.

For Smart Yield clients, the execution boundary is separate and clear. Engineering on-chain bots evaluate on-chain conditions and trigger actions for Smart Yield controls. The Risk Application supports the governance side of this process by documenting the framework relationship, exposing trigger settings, publishing configuration state, and preserving the reporting context. This gives Sentora one control narrative across application infrastructure and on-chain execution infrastructure.

The fourth monitoring layer is risk alert aggregation. The Risk Alerts dashboard collects alerts across registered modules and summarizes critical, warning, and informational signals. The current alert configuration defines 17 modules and 458 threshold keys. These modules cover daily risk, client breaches, weekly risk, interest rates, market data, protocol vaults, Hypernative, DD versioning and external vaults.

Figure 7: Risk alert aggregation

Risk Alert Summary

Aggregated risk alerts from all platform modules

Refresh

Alerts Configuration

6 Critical 25 Warning

All Critical Warning Info

> Daily Risk (T-0 vs T-1) 1 alert Stale Data: 2026-06-08

> Protocol Vault Config OK Data: 2026-06-08

> Maple Finance 3 alerts Data: 2026-06-08

> Figure Markets — Solana 2 alerts Data: 2026-06-08

> Hypernative Security OK Data: 2026-06-09T12:50:32.677580+00:00

> Ethena Protocol 20 alerts Data: 2026-06-08

> Figure Markets — Ethereum 5 alerts Data: 2026-06-08

The fifth monitoring layer is real-time security ingestion. The Hypernative integration receives webhook alerts, validates signatures, normalizes alert payloads, classifies severity, and surfaces alerts in the Hypernative dashboard.

The sixth monitoring layer is data health. Data health checks confirm whether source data is fresh, complete, and structurally stable. The production database evidence snapshot contains 1,630 data health checks, 1,596 record count history rows, and 16 schema snapshots. These counts show that Sentora monitors the monitoring infrastructure itself.

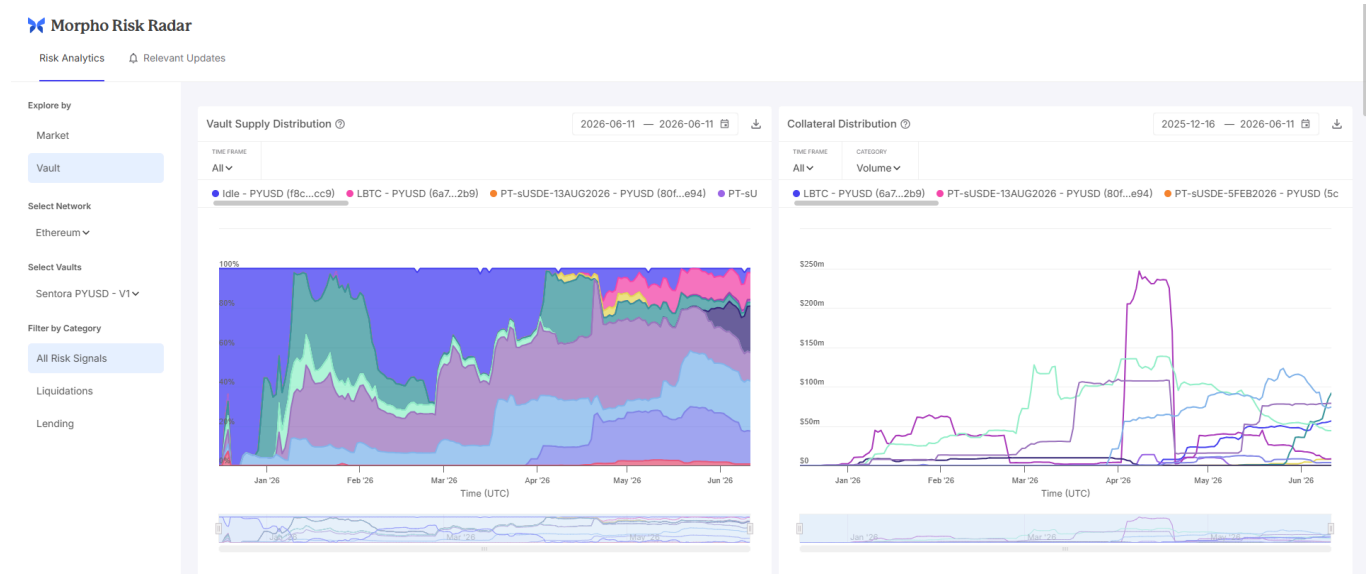
Monitoring Evidence

Monitoring area	Operating signal
Risk alert modules	17
Risk alert threshold keys	458
Hypernative alerts in production snapshot	2
Hypernative webhook log rows	6
Data health checks	1,630
Data health record count history rows	1,596
Data health schema snapshots	16

Risk Radar

The analytics foundation beneath these monitoring layers is Risk Radar, Sentora's proprietary risk analytics platform. Risk Radar tracks protocol, vault, and market health through economic risk signals computed block by block from on-chain data, covering more than 40 protocols with hundreds of indicators designed around each protocol's specific mechanics and failure modes. At the protocol level it measures solvency and structural stability through signals such as health factor distribution, bad debt, liquidation activity, reserve metrics, and peg deviation. At the vault level it tracks utilization, collateral composition, and loans at risk of liquidation. At the market level it monitors DEX liquidity depth, exit cost, net liquidity flows, whale concentration, and volatility distribution.

Risk Radar is what turns the controls described in this chapter into advanced risk analysis rather than static reporting. The thresholds enforced by the alert collectors, the parameter baselines used in protocol vault monitoring, and the trigger logic behind the daily jobs all draw on the same signal layer, and the Risk Pulse anomaly detection engine scans it continuously for statistically meaningful deviations. Because the signals are available programmatically as well as through dashboards and alerts, the risk team can analyze conditions historically for due diligence, monitor them live for position management, and aggregate them across deployments for portfolio oversight. These are the same analytics Sentora uses to manage its own strategies, and they exist to make one principle operational: return of capital before return on capital.



6. Reporting, Escalation, And Governance Closure

Sentora connects alerts, reports, access controls, protocol communication, issuer communication, and Risk Committee review so that risk events move from detection into documented action.

The first response is direct communication. For protocols and asset issuers approved for the Sentora ecosystem, Sentora maintains dedicated communication channels with the relevant teams. When an issue or alert arises, the first step is to contact the protocol or issuer directly, verify the facts, and assess whether the event requires parameter review, exposure adjustment, client communication, or escalation.

For larger incidents, Sentora uses [PagerDuty](<https://www.pagerduty.com/>) as part of its incident response infrastructure. PagerDuty brings the relevant team members online and supports Sentora's war-room setup for coordinated response. This process is used when an event is broader than a single alert, affects multiple exposures, or requires cross-functional coordination across risk, research, engineering, operations, and client-facing teams.

The first closure layer is daily reporting. Daily reports summarize position analysis, token concentration, trade flow, executive summary data, unified risk views, TVL data, client-specific filtered reports, collateral health, and protocol configuration changes. Each report links current observations to prior observations, which gives the risk team a structured record of how exposure changed between T-0 and T-1.

Figure 8: Daily risk report archive

Daily Risk Reports

Latest report: June 08, 2026

REPORTS AVAILABLE

30 days

579 main reports, 996 specific client reports

Recent Reports

June 08, 2026

24 + 42 reports

REPORT	TYPE	SIZE	GENERATED	ACTION
exec_summary_daily_20260608_151733.html HTML	Executive Summary	69.8 KB	5:17:33 PM	View
exec_summary_daily_20260608_225539.html HTML	Executive Summary	69.8 KB	12:55:39 AM	View
sentora_report.html HTML	Unified Analysis	94.1 KB	5:17:20 PM	View
sentora_report_225542.html HTML	Unified Analysis	94.5 KB	12:55:28 AM	View
trade_analysis_20260608_151725.html HTML	Trade Analysis	439.1 KB	5:17:27 PM	View
trade_analysis_20260608_225532.html HTML	Trade Analysis	439.2 KB	12:55:34 AM	View
weekly_risk_checkpoints_20260608.html HTML	Weekly Risk	79.3 KB	5:17:36 PM	View

The second closure layer is report organization and access. The Daily Risk dashboard lists recent report dates, report families, pinned reports, available reports, hidden reports, and specific client reports. Slack-linked reports use a daily rotating report key derived from the cloud service combined with the calendar date. Persistent access stays inside the authenticated application.

The third closure layer is escalation. The framework uses clear severity levels. Info events are logged and visible on dashboards. Warning events notify the risk team and increase monitoring. Breach events trigger immediate email alerting and require a formal incident report within 24 hours. Critical events move to Risk Committee escalation and corrective action, including position reduction or unwind where required.

The fourth closure layer is periodic governance. Weekly checkpoints provide trend analysis across the prior period. Monthly reports support client review, mandate compliance, strategy review, and deviation analysis. Framework changes are governed by the Risk Committee and reviewed annually or upon material ecosystem change.

The fifth closure layer is auditability. Report files, job statuses, data health histories, DDQ dossiers, protocol configurations, alert records, and configuration overrides combine to form a continuous review trail. That trail is what makes vault curation defensible, because curation depends on evidence of two things: decision quality and operating discipline. It lets Sentora show the diligence record behind each choice, the approved policy that governs it, the active control that enforces it, the monitoring output that tracks it, and the response path that resolves any issue.

Production evidence supports this reporting layer. The Sentora Risk Application database volume contains 21,931 report files. The largest report families are hybrid-fund reports, daily-risk reports, vault-client reports, external-vault reports and interest-rate reports. This shows that reporting is a continuous operating output across the same infrastructure that runs monitoring and alerts.

This final stage closes the front-to-back chain. Each layer builds on the one before it. The DDQ defines eligibility, while the framework defines acceptable exposure. Controls translate that policy into enforceable limits, and monitoring tests those limits against current data. Reporting, governance, and escalation then turn monitoring into disciplined action.

Figure 9: Governed report display settings

Report Display Settings

Configure which reports are pinned, available, or hidden on the Daily Risk dashboard

Three-Tier Report Visibility

Pinned

 reports are always visible at the top — your daily must-reads.

Available

 reports are collapsed under "More Reports" — click to expand.

Hidden

 reports are tucked behind "Show all files" — raw data and legacy files.

Display Rules

Custom OverrideUpdated: 2026-02-23T23:52:03

Default tier for unmatched reports: AvailableApplied when no rule matches a report's type and extension

REPORT TYPE	EXTENSION	TIER	MATCHES
exec_summary	.html	Pinned	exec_summary .html files
detailed_position	.html	Available	detailed_position .html files
token_analysis	.html	Available	token_analysis .html files
trade_analysis	.html	Pinned	trade_analysis .html files
weekly_risk	.html	Pinned	weekly_risk .html files
other	.txt	Hidden	.txt files not matched by a specific type
sentora_unified	*	Pinned	All sentora_unified files (any extension)

Escalation Map

Severity	Trigger	Response
Info	Normal metrics remain within range.	Logged and visible on dashboard.
Warning	A threshold is approached.	Risk team review and increased monitoring.
Breach	A client restriction or critical threshold is violated.	Immediate email alert and formal incident report within 24 hours.
Critical	Active threat, liquidation risk, or material control breach.	Risk Committee escalation and corrective action.

Reporting Evidence

Reporting area	Production signal
Production report files	21,931
Daily-risk report files	7745
External-vault report files	487
Hybrid-fund report files	9963
Treasury report files	442
Vault-client report files	3293
Daily reporting cadence	Specific time UTC daily
Monthly client report cadence	Specific time CET, first day of month

Conclusion

Sentora's vault risk model is front to back by design. It starts before deployment through DDQ intake and evidence review and continues through a risk framework that distinguishes Sentora-Vaults, Smart Yield clients, and Protocol-Vaults. It becomes operational through mandates, protocol vault configs, LLTV and cap controls, trigger thresholds, monitoring, alerts, reports, and governance.

This structure is important because vault risk changes during operation. A review at onboarding is only the first control. The operating requirement is a governed system that can approve exposure, constrain deployment, monitor current state, identify breaches, and preserve the record of response.

Sentora has built that system as infrastructure. The Risk Application is the evidence surface for diligence, policy, controls, monitoring, reporting, and escalation. Engineering on-chain bots extend that control model for Smart Yield clients. Together, the application layer and execution layer create a disciplined operating model for capital deployment under real market conditions.

Source Notes

1. Sentora framework sources include `docs/RFP_Risk_Management_Framework_Overview.md`, `docs/Risk Framework - Sentora Vaults.pdf`, `docs/Risk Framework - Protocol Vaults.pdf`, and `docs/SALES_USER_GUIDE.md`.
2. DDQ sources include `docs/manuals/risk_ddq_manual.md`, `vault-clients/app/routes/risk_ddq.py`, and the Risk DDQ dashboard screenshot in Figure 3.
3. Control and monitoring sources include `vault-clients/app/routes/client_config.py`, `vault-clients/app/routes/protocol_vaults.py`, `vault-clients/app/routes/risk_triggers.py`, `vault-clients/app/risk_alerts/collectors/protocol_vaults.py`, and the protocol-specific collateral fetchers for Euler, Kamino, and Morpho.
4. Smart Yield execution context is based on the active trigger configuration in `data/config/protocol_vault_triggers.json`, the risk trigger dashboard, and user confirmation that engineering on-chain bots execute Smart Yield on-chain controls outside the Risk Application.
5. Reporting and governance sources include `vault-clients/app/routes/reports.py`, `vault-clients/app/routes/report_settings.py`, the daily report archive screenshot in Figure 8, and the report settings screenshot in Figure 9.
6. Production evidence was captured on 2026-05-29 from Railway through the admin-only aggregate evidence endpoint. The endpoint returns aggregate counts and excludes raw DDQ text, alert payloads, client records, vault addresses, and secrets.
7. Sentora public research context comes from [Sentora Research](#), [Sentora Research Reports](#), and the report mapping maintained in `docs/research/2026-05-29-front-to-back-vault-risk-management-draft.md`.