QUANTIFIND

The Buyer's Guide to Modern Sanctions Screening

Eight capabilities financial institutions should evaluate to move from potential matches to meaningful risk decisions.

Executive Summary

Sanctions screening is no longer simply a matter of comparing customer and payment names against government watchlists.

Financial institutions now need to manage sanctions data from numerous sources, resolve entities across languages, uncover indirect ownership and control, evaluate complex relationships, monitor changing exposure, and make defensible decisions before funds move. Legacy screening systems, built largely around static records and alert generation, often struggle to provide that context.

Sanctions leaders themselves are signaling that the traditional operating model is under pressure. In practitioner polling reported through 1LoD's 2026 Financial Crime Summit research, 52% of financial crime leaders said their function was not fit for the future, compared with only 33% who believed it was. The same research found that sanctions had experienced more change from geopolitical developments than any other financial crime discipline during the preceding year.

For institutions evaluating sanctions technology, the question is no longer simply:

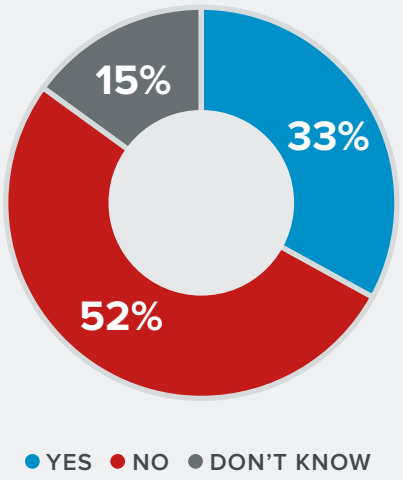
Can the system find a potential match?

The more important question is:

Can the platform determine whether that match represents meaningful risk, and provide the context and evidence needed to act?

This buyer's guide outlines eight capabilities financial institutions should evaluate when selecting a modern sanctions platform. It also provides practical questions and criteria to use during vendor demonstrations, proof-of-concept testing, and RFPs.

I believe that my organization's financial crime function is fit for the future.



In practitioner polling reported through 1LoD's 2026 Financial Crime Summit research, **52%** of financial crime leaders said their function was not fit for the future, compared with only **33%** who believed it was. The same research found that sanctions had experienced more change from geopolitical developments than any other financial crime discipline during the preceding year.

At a Glance:

Your Sanctions Technology Evaluation Checklist

Use this checklist as you evaluate sanctions technology providers. A modern platform should do more than aggregate sanctions lists or generate potential matches. It should help your institution normalize source data, resolve identities, understand ownership and relationships, monitor changing risk, and support faster, explainable decisions.

The eight capabilities below provide a practical framework for comparing solutions. **Each is explored in greater detail later in this guide, including what to look for and the questions to ask prospective vendors.**

- [ ] **Sanctions List Management**
  Continuously ingest, normalize, and reconcile sanctions and watchlist data while creating a unified view of entities across multiple sources.
- [ ] **Accurate, Multilingual Entity Resolution**
  Resolve people and organizations accurately across aliases, transliterations, languages, and other identity variations.
- [ ] **Beneficial Ownership and Control Analysis**
  Identify direct and indirect ownership, control, and connections to sanctioned parties.
- [ ] **Network and Relationship Intelligence**
  Reveal meaningful relationships among people, companies, vessels, counterparties, and other entities.
- [ ] **Real-Time Customer and Payment Screening**
  Support accurate, prioritized decisions at the speed modern payments require.
- [ ] **Continuous Monitoring and Current Risk Intelligence**
  Identify material changes in sanctions exposure as relationships, ownership, and geopolitical conditions evolve.
- [ ] **Explainable, Evidence-Backed Decisions**
  Show why risk was identified and provide the underlying evidence needed for review, governance, and audit.
- [ ] **Integration Without Unnecessary Replacement**
  Add intelligence to existing screening, payment, and case-management environments without automatically requiring wholesale replacement.

Keep this checklist handy as you move through the guide and during vendor demonstrations, proof-of-concept testing, and RFP evaluations.

Why Traditional Sanctions Screening Is Falling Behind

Traditional sanctions screening systems were generally designed around a predictable process:

1. Collect sanctions and watchlist data.
2. Resolve people and organizations accurately across aliases, transliterations, languages, and other identity variations.
3. Generate alerts based on matching rules.
4. Send potential matches to analysts for review.
5. Clear or escalate each alert.

That model remains necessary, but it is no longer sufficient.

Sanctions risk may be hidden behind aliases, transliterations, incomplete records, shell companies, beneficial owners, intermediaries or complex corporate structures. An apparently legitimate company may be owned or controlled by a sanctioned party without appearing on a sanctions list itself.

At the same time, geopolitical events, sanctions designations, export controls, and trade restrictions can change an institution's exposure quickly. Periodic screening and static customer records may not capture these changes soon enough.

1LoD's research characterizes the current environment as one of sustained volatility rather than episodic disruption. New sanctions can emerge with little warning. Regional requirements may diverge. Export controls can evolve rapidly, and institutions must translate those changes into consistent controls across jurisdictions and business lines.

Why Traditional Sanctions Screening Is Falling Behind

This creates a difficult combination of challenges:

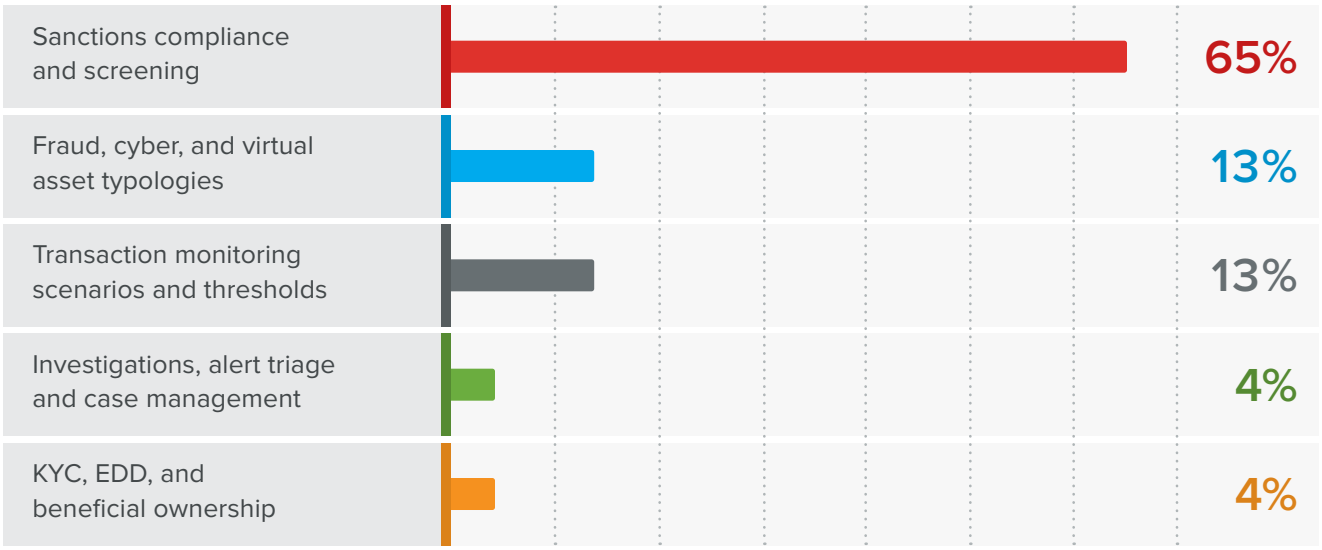
- **High volumes of false positives** that consume analyst time and delay legitimate activity
- **Meaningful risk hidden beyond the initial match** because identity, ownership, or relationship context is incomplete
- **Slow, manual investigations** that require analysts to gather evidence across multiple systems
- **Limited visibility into indirect ownership and control**
- **Difficulty understanding complex networks** involving counterparties, intermediaries, companies, vessels, and other connected entities
- **Fragmented customer, payment, and external-risk data**
- **Risk that changes after onboarding** because of new designations, ownership changes, relationships, or geopolitical developments
- **Pressure to screen real-time payments without creating unnecessary delays**
- **Inconsistent decisions across teams, business lines, and jurisdictions**
- **Insufficient evidence to explain why an alert was cleared, prioritized, or escalated**

The concern extends beyond individual screening systems. In a separate report from its Financial Crime Leaders' Network, 1LoD found broad agreement among senior practitioners that integration across AML, KYC, fraud and sanctions was both desirable and inevitable. Participants also emphasized that progress remained incremental and uneven—and was more advanced at the data layer than at the organizational level.

That is an operating-model problem, not merely a watchlist problem.

→ Why Traditional Sanctions Screening Is Falling Behind

Which area of your firm has changed most in the last 12 months due to geopolitical developments?



Adding more analysts to review more alerts does not address the underlying issue. The goal should not be to generate fewer alerts. It should be to help institutions distinguish **potential matches from meaningful risk**, and give analysts the context and evidence needed to make that distinction confidently.

Geopolitical Volatility Has Changed the Sanctions Operating Model

Financial crime programs have always responded to geopolitical events. What has changed is the speed, breadth and persistence of that change.

A single geopolitical development can alter:

- Customer risk
- Counterparty risk
- Payment risk
- Trade and export-control risk
- Supply-chain exposure
- Product strategy
- Cross-border operations
- Regulatory expectations

Traditional programs were built for an environment in which lists changed, systems refreshed, alerts were reviewed, and controls were recalibrated on a relatively predictable cycle. They were not designed for an environment in which multiple dimensions of risk can change simultaneously.

Technology alone will not create an adaptable sanctions program. Institutions also need governance, risk assessment, internal controls, testing, training, and senior-management commitment. The U.S. Treasury's Office of Foreign Assets Control identifies those elements as essential components of an effective sanctions compliance program in its *Framework for OFAC Compliance Commitments*.

The Wolfsberg Group similarly treats screening as one element within a broader sanctions compliance program. Its guidance asks financial institutions to evaluate screening effectiveness in light of the growing complexity of international sanctions requirements.

For technology buyers, the implication is clear:

Sanctions screening should not be evaluated as an isolated list-matching utility.

What Is AI-Native Sanctions Screening?

Not every use of AI in sanctions screening represents the same approach.

AI can be added to a traditional screening workflow to improve individual tasks. An **AI-native approach** goes further. Capabilities such as entity resolution, contextual intelligence, and relationship analysis are foundational to how the platform identifies and evaluates risk.

A modern AI-native sanctions platform should help an institution determine:

- How to manage the changing sanctions being imposed
- Who the customer, counterparty, or beneficiary actually is
- Whether different records refer to the same person or organization
- Whether an entity is owned or controlled by a sanctioned party
- Whether hidden relationships create indirect sanctions exposure
- Whether transaction, trade or adverse-media context changes the risk
- Whether an alert should be cleared, prioritized or escalated
- What evidence supports the resulting decision

These capabilities extend screening beyond name similarity and toward a fuller understanding of the entity and its surrounding risk.

The objective is not to replace sanctions analysts with a black-box model. It is to give analysts and operational systems better evidence, reduce unnecessary work and make decisions more consistent.

AI should strengthen human judgment by resolving entities, organizing relevant information, and explaining why a particular risk was identified.

That distinction is important. The Financial Action Task Force's risk-based approach calls on financial institutions to identify, assess and understand their risks, then apply controls proportionate to those risks. A mechanical match score does not, by itself, provide that understanding.

Eight Capabilities to Look for in Sanctions Screening Software

1. Sanctions "List" Management

Financial institutions typically need to screen against hundreds of sanctions, watchlist, law-enforcement, and regulatory sources.

Depending on the institution's jurisdiction and risk profile, those sources can include:

- OFAC (U.S.)
- UN Security Council
- EU Consolidated List
- UK OFSI
- National sanctions lists from Canada, Australia, Japan, Singapore, etc.
- Law enforcement and regulatory watchlists

The challenge is that these sources do not necessarily describe people, companies, and other entities in the same way.

Lists can differ in their:

- Naming conventions
- Languages and transliterations
- Aliases
- Data quality
- Update frequency
- Entity identifiers

Simply combining sanctions lists can create duplication and increase the burden on downstream screening. A modern approach should treat each list as an independent source, while creating a unified view of entities represented across those sources.

→ Eight Capabilities to Look for in Sanctions Screening Software

1. Sanctions List Management

Raw sanctions data	What a modern platform should do
Duplicate entries across multiple lists	Resolve them into a single entity profile
Different spellings and transliterations	Recognize variants as the same person or company
Fragmented attributes	Combine aliases, addresses, IDs, countries, dates of birth, and corporate information into one explainable profile
Multiple independent sanctions hits	Produce one consolidated risk assessment with supporting evidence
Isolated list entries	Place the entity into a broader network of ownership and relationships

This entity-centric approach helps reduce duplicate alerts while improving matching accuracy across multilingual names, aliases, and other identity variations.

ENRICHMENT BEYOND SANCTIONS LISTS

List data alone may not provide enough context to understand the risk associated with an entity.

Depending on the use case, a modern platform may enrich sanctions data with information such as:

- Corporate registry information
- Beneficial ownership
- Subsidiary hierarchies
- Trade relationships
- Adverse media
- Regulatory filings
- Other public and commercial intelligence

The goal is to help an analyst understand **why** an entity may present risk—not just that it appears on a list.

→ Eight Capabilities to Look for in Sanctions Screening Software

1. Sanctions List Management

CONTINUOUS NORMALIZATION

Sanctions authorities continuously add, remove, and update records.

A modern solution must be able to ingest and normalize changing data so institutions do not have to manually reconcile differences in formats, identifiers, aliases, or other attributes every time a source is changed.

This is more than combining sanctions lists. It means:

- **Normalizing** disparate data from many sanctions sources.
- **Resolving** duplicate and variant identities into unified entities.
- **Enriching** those entities with contextual and relationship data.

WHAT GOOD LOOKS LIKE

Buyers should look for a platform that can preserve the provenance of individual list sources while creating an explainable, unified view of the underlying entity.

ASK POTENTIAL VENDORS:

- [ ] Which sanctions, watchlist, and restricted-party sources do you support?
- [ ] How are list changes collected, validated, and delivered?
- [ ] How do you identify duplicate or overlapping records across sources?
- [ ] How do you preserve the original source and designation information after records are resolved?
- [ ] How do you handle conflicting or incomplete attributes across lists?
- [ ] What additional intelligence can be used to enrich sanctions records?
- [ ] How quickly are source changes reflected in the platform?

→ Eight Capabilities to Look for in Sanctions Screening Software

2. Accurate, Multilingual Entity Resolution

Entity resolution determines whether records from different sources refer to the same real-world person or organization.

This is essential because names may appear with:

- Alternative spellings
- Aliases
- Abbreviations
- Transliterations
- Reversed name order
- Missing identifiers
- Inconsistent corporate suffixes
- Native and non-Latin characters
- Typographical errors

A screening system that relies primarily on character similarity may generate excessive false positives while still missing genuine relationships.

Better entity resolution can improve both sides of screening performance by reducing irrelevant matches while increasing confidence in genuine ones.

WHAT GOOD LOOKS LIKE

The platform should use identity attributes and contextual evidence to determine whether records refer to the same real-world entity, rather than simply comparing strings.

ASK POTENTIAL VENDORS:

- [ ] Does the platform resolve people and companies—not merely compare strings?
- [ ] Can it distinguish two people with similar names using contextual attributes?
- [ ] How does it handle aliases, transliteration and non-Latin scripts?
- [ ] Can it connect fragmented internal and external records?
- [ ] Does it show the evidence behind its entity-resolution decision?

3. Beneficial Ownership and Control Analysis

A company does not need to appear directly on a sanctions list to create sanctions exposure.

Financial institutions may need to determine whether it is directly or indirectly owned or controlled by a sanctioned person or entity. That analysis can require examining multiple corporate layers, shareholders, directors, affiliates and other relationships.

A modern sanctions compliance platform should be able to:

- Identify direct and indirect ownership
- Traverse corporate hierarchies
- Reveal beneficial owners and controlling parties
- Show the path connecting an entity to a sanctioned party
- Detect relationships involving shell companies or intermediaries
- Monitor ownership structures for material changes

The system should not simply return an ownership flag. It should present the relationship in a form an analyst can understand, validate and document.

This capability is becoming more important as sanctions and export controls increasingly overlap. Financial institutions may need to determine whether goods are being diverted through intermediary countries, whether a customer's supply chain creates hidden exposure, or whether an apparently legitimate counterparty is connected to a restricted party.

WHAT GOOD LOOKS LIKE

Buyers should look for a platform that can move beyond direct list exposure and show both the ownership structure and the evidence connecting an entity to a sanctioned or restricted party.

ASK POTENTIAL VENDORS:

- [ ] Can the platform identify both direct and indirect ownership?
- [ ] How many layers of corporate ownership can it analyze?
- [ ] Can analysts see the complete relationship path to a sanctioned party?
- [ ] How does the platform distinguish ownership from control?
- [ ] How frequently is ownership information refreshed?
- [ ] Can changes in ownership trigger ongoing monitoring or reassessment?

→ Eight Capabilities to Look for in Sanctions Screening Software

4. Network and Relationship Intelligence

Many sanctions-evasion risks only become visible when entities are evaluated as part of a network.

A customer may interact with apparently unrelated companies that share directors, addresses, beneficial owners, vessels, trading partners or other attributes. Intermediaries may be used to obscure the ultimate beneficiary, destination or source of funds.

Network analysis can help financial institutions uncover:

- Hidden connections between counterparties
- Shared ownership or management
- Layers of intermediary companies
- Potential diversion pathways
- Relationships with restricted jurisdictions
- Clusters of connected high-risk entities
- Previously unknown exposure beyond the initial alert

For institutions exposed to trade and maritime sanctions, evaluating a vessel name in isolation may not provide enough context.

Buyers should consider whether a platform can connect vessels with relevant entities and relationships, including owners, operators, companies, counterparties, and other associated parties.

The objective is to help analysts understand exposure that may not be apparent from the initial vessel or company match.

The broader question is not simply whether a vessel or related company produces a match.

It is whether the platform can reveal the network surrounding that match and help the institution understand the resulting risk.

WHAT GOOD LOOKS LIKE

The platform should help analysts move beyond the initial match and understand the network surrounding an entity, including the evidence and relationship paths that make those connections relevant.

ASK POTENTIAL VENDORS:

- [ ] Can the platform identify relationships beyond direct ownership?
- [ ] Which entity and relationship types can it analyze?
- [ ] Can analysts visually trace the path between connected entities?
- [ ] Can it identify shared attributes that connect apparently unrelated parties?
- [ ] Does network analysis extend to vessels and maritime relationships where relevant?
- [ ] How does the platform distinguish meaningful relationships from incidental connections?

→ Eight Capabilities to Look for in Sanctions Screening Software

5. Real-Time Customer and Payment Screening

Real-time payments place sanctions decisions directly in the transaction flow.

When funds move within seconds, an institution may not have time to place every ambiguous result into a lengthy manual-review queue. The screening platform must produce accurate, prioritized, and explainable intelligence quickly enough to support an operational decision.

Yet industry readiness remains limited. In the 1LoD practitioner research, only 9% of organizations reported having effective real-time monitoring and interdiction controls in place. Most respondents expected implementation to take years.

That gap exposes the limits of an alert-centric model. Generating more alerts is not an effective response when the business must make a decision in seconds.

WHAT GOOD LOOKS LIKE

Real-time screening should combine speed with accurate identity resolution, contextual risk information, explainability, and operational resilience.

“Real time” should be defined through measurable service levels, rather than used as a general marketing term.

ASK POTENTIAL VENDORS:

- [ ] What is the screening latency under realistic transaction volumes?
- [ ] What availability and resilience commitments are provided?
- [ ] Which payment formats and data are supported?
- [ ] How does the system handle incomplete payment information?
- [ ] Can thresholds be configured according to institutional risk appetite?
- [ ] How does the solution integrate with payment and case-management systems?
- [ ] What is the workflow for hold, release, reject, and escalate decisions?

→ Eight Capabilities to Look for in Sanctions Screening Software

6. Continuous Monitoring and Current Risk Intelligence

A customer that presented acceptable risk during onboarding may become exposed later because of a new designation, ownership change, geopolitical event or newly discovered relationship.

Modern sanctions screening software should therefore support continuous monitoring rather than relying solely on periodic rescreening.

Continuous monitoring can help identify:

- New sanctions designations
- Changes in ownership or control
- New high-risk relationships
- Emerging adverse information
- Changes in geography or trading activity
- New export-control or restricted-party exposure
- Material changes requiring customer reassessment

WHAT GOOD LOOKS LIKE

The institution should be able to define which changes are material, determine which customers or counterparties are affected, and establish how those changes should affect downstream workflows.

The objective is not simply to receive more alerts every time data changes. It is to identify the changes that meaningfully affect risk.

ASK POTENTIAL VENDORS:

- [ ] Which changes can trigger ongoing monitoring?
- [ ] How quickly is new sanctions or risk information incorporated?
- [ ] Can monitoring identify new relationships as well as new list designations?
- [ ] Can the institution define what constitutes a material change?
- [ ] How are affected customers or counterparties prioritized for review?
- [ ] How does monitoring integrate with downstream case-management workflows?

→ Eight Capabilities to Look for in Sanctions Screening Software

7. Explainable, Evidence-Backed Decisions

Explainability is essential in a regulated sanctions environment.

Analysts, reviewers, auditors and regulators may need to understand:

- Why the system produced a match
- Which attributes influenced the result
- Which entities and relationships were identified
- Which original sources support the finding
- Why an alert was cleared or escalated
- Where human judgment entered the process
- Whether the decision followed institutional policy

A model score by itself is not a sufficient explanation.

WHAT GOOD LOOKS LIKE

Look for a platform that provides evidence provenance, source links, relationship paths, configurable reasoning, and a complete audit trail. The institution should be able to reproduce the basis for a decision after it has been made.

Explainability is not simply a technical feature. It can also support the risk assessment, internal controls, and testing expected within an effective sanctions compliance program.

ASK POTENTIAL VENDORS:

- [ ] Can an analyst see why a match was generated?
- [ ] Can the platform show which attributes and relationships influenced the result?
- [ ] Is original source evidence available?
- [ ] Can analysts reproduce the basis for a historical decision?
- [ ] Is human review captured in the audit trail?
- [ ] Can the institution configure decision logic to reflect its policies and risk appetite?

→ Eight Capabilities to Look for in Sanctions Screening Software

8. Integration Without Unnecessary Replacement.

Many institutions already have sanctions lists, transaction-monitoring systems, payment controls and case-management platforms in place.

A modernization initiative should not automatically require a complete replacement of that infrastructure.

An AI-native risk intelligence layer can improve an existing environment by:

- Enriching alerts with external intelligence
- Resolving customers and counterparties
- Prioritizing meaningful risks
- Suppressing clearly irrelevant results within approved controls
- Revealing ownership and network relationships
- Delivering structured evidence to existing workflows
- Supporting screening through synchronous or batch APIs
- Enabling continuous monitoring across the customer population

The industry's integration challenge extends beyond technology. When 1LoD asked practitioners about their greatest challenges in managing sanctions across jurisdictions, 50% cited aligning global policies with local implementation, 25% cited keeping lists and reference data current, 15% cited conflicting regulatory requirements, and 10% cited technology and system limitations.

WHAT GOOD LOOKS LIKE

Buyers should understand what the solution can augment, what must be replaced, and how it will operate within existing governance, architecture, workflows, and risk appetite.

ASK POTENTIAL VENDORS:

- [ ] Which existing systems can the platform augment?
- [ ] Which components, if any, must be replaced?
- [ ] Which APIs, batch processes, and native integrations are available?
- [ ] Can intelligence be delivered into existing analyst and case-management workflows?
- [ ] How much implementation effort is typically required?
- [ ] How does the platform operate within existing governance and risk controls?

Traditional Screening Versus an AI-Native Sanctions Platform

Evaluation Area	Traditional screening approach	AI-native sanctions approach
Identity matching	Compares names using fixed or fuzzy rules	Resolves real-world entities using names, attributes and contextual evidence
Multilingual coverage	Relies heavily on standardized or translated names	Evaluates aliases, transliterations and native-language variations
Ownership risk	Focuses primarily on directly listed entities	Analyzes direct and indirect ownership, control and corporate relationships
Risk context	Uses sanctions-list data as the principal signal	Incorporates corporate, adverse-media, trade and network intelligence
Monitoring	Rescreens on a periodic schedule	Continuously evaluates material changes
Alert handling	Sends possible matches to manual review	Prioritizes alerts using identity and contextual risk
Investigations	Requires analysts to gather evidence from separate systems	Delivers resolved entities, relationships and supporting evidence together
Explainability	Provides a match score or rule result	Shows why the risk was identified and which evidence supports the decision
Operating model	Functions as a standalone screening control	Supplies risk intelligence across KYC, payments, investigations and trade

Buyer Toolkit: How to Evaluate an AI Sanctions Screening Vendor

Vendor demonstrations often use clean data and straight-forward examples. A meaningful evaluation should test the platform against the institution's actual risks and operating conditions.

Put the Platform to the Test

A proof of concept should include difficult cases involving:

- Common names
- Limited identifiers
- Multiple languages and scripts
- Aliases and transliterations
- Complex corporate ownership
- Indirect sanctions exposure
- Intermediary organizations
- High-volume customer screening
- Realistic payment messages
- Known true positives and known false positives
- Previously investigated alerts

Do not limit a demonstration to whether the platform can find a match.

Ask vendors to show **how the platform determines what the match means.**

→ Buyer Toolkit: How to Evaluate an AI Sanctions Screening Vendor

Establish Your Metrics Before Testing

The institution should define its evaluation metrics before testing begins.

Useful measures include:

- Recall against known true matches
- Precision and false-positive rate
- Entity-resolution accuracy
- Detection of indirect ownership and control
- Performance across languages and scripts
- Payment-screening response time
- Analyst review time
- Evidence completeness
- Consistency between reviewers
- Alert reduction under approved risk thresholds
- Integration effort
- Auditability and decision reproducibility

Any claim about alert reduction or accuracy should be evaluated against a clearly defined baseline. A high percentage is not meaningful unless the institution understands the data, thresholds, population, and decision criteria behind it.

The goal is not simply to automate more activity. It is to improve outcomes by identifying risk earlier, avoiding unnecessary investigations, releasing legitimate payments faster, and adapting more consistently when conditions change.

Questions to Include in a Sanctions Screening RFP

Financial institutions should ask prospective vendors:

1. How does your platform distinguish entity resolution from fuzzy name matching?
2. Which sanctions, watchlist and restricted-party data sources are supported?
3. How are list changes collected, validated and delivered?
4. How does the system handle aliases, transliteration and non-Latin scripts?
5. Can the platform identify direct and indirect ownership and control?
6. How are ownership and network relationships presented to analysts?
7. What evidence explains each match, clearance and escalation?
8. How does the platform support real-time payment screening?
9. What throughput and latency commitments are available?
10. Can thresholds be configured by jurisdiction, business line and risk appetite?
11. How does continuous monitoring identify and prioritize material changes?
12. Can the solution enrich existing screening or case-management platforms?
13. What APIs, batch processes and native integrations are available?
14. How is customer data protected, retained and segregated?
15. How are models validated, tested, monitored and governed?
16. How does the platform preserve human review and approval?
17. Can the vendor test performance using the institution's own scenarios?
18. How are model, data and configuration changes recorded for audit purposes?

How Quantifind Approaches Modern Sanctions Compliance

The practitioner evidence points toward a sanctions operating model that must be more connected, contextual and adaptable.

Quantifind's AI-native Risk Intelligence Platform is designed to support that transition by helping financial institutions move beyond static name matching and understand sanctions risk in context.

The platform combines:

- **Name Science**™ to evaluate name variations, aliases and transliterations across languages
- **AI-driven entity resolution** to connect fragmented records and identify the correct person or organization
- **Ownership and relationship analysis** to reveal indirect exposure and hidden control
- **Deep network analysis** to identify connections, intermediaries and risk patterns
- **Dynamic risk typologies** to detect evolving sanctions and financial-crime risks
- **Continuously refreshed external intelligence** to monitor changing exposure
- **Explainable, evidence-backed results** to support analysts, governance and audit requirements
- **Flexible integration options** to deliver intelligence into existing screening, transaction-monitoring and case-management workflows

Rather than treating sanctions screening as an isolated alert-generation process, Quantifind supplies trusted risk intelligence across customer onboarding, ongoing monitoring, payments, investigations, trade and enterprise financial-crime operations.

The objective is straightforward: help institutions identify genuine sanctions risk more accurately, reduce avoidable compliance friction and make faster, more defensible decisions.

Frequently Asked Questions

What is the difference between sanctions screening and entity resolution?

Sanctions screening compares a customer, counterparty or payment against sanctions and restricted-party data. Entity resolution determines which real-world person or organization a record represents. Accurate entity resolution improves screening by distinguishing genuine matches from people or companies with similar names.

Can AI sanctions screening reduce false positives?

AI can reduce false positives when it evaluates identity attributes, relationships and risk context rather than relying primarily on name similarity. Results depend on data quality, model performance, configuration and the institution's risk appetite, so reduction claims should be validated using realistic data.

Can sanctions software identify beneficial ownership?

Advanced sanctions platforms can analyze corporate hierarchies and ownership relationships to identify direct and indirect connections to sanctioned parties. Buyers should confirm the depth, freshness and geographic coverage of the vendor's ownership data.

How is AI used in real-time payment screening?

AI can resolve counterparties, assess contextual risk and prioritize potential matches within the payment workflow. The platform must still meet the institution's requirements for latency, resilience, explainability, governance and human escalation.

Should a financial institution replace its existing screening system?

Not necessarily. An institution may be able to add an intelligence and entity-resolution layer to improve an existing screening environment. The correct approach depends on current-system performance, integration capabilities, operational risk and modernization objectives.

What makes an AI sanctions decision explainable?

An explainable result shows which entity was identified, what attributes and relationships influenced the finding, which sources support it and how the result maps to policy. It should provide more than a match score and preserve a reproducible audit trail.

Move From Potential Matches to Better Sanctions Decisions

The future of sanctions compliance is not defined by longer watchlists or larger alert queues.

It is defined by the ability to identify entities accurately, uncover indirect exposure, understand risk in context, and deliver explainable decisions across the financial crime lifecycle.

The evidence from sanctions and financial crime leaders makes the urgency clear:

- **52%** said their financial crime function was not fit for the future.
- Sanctions had experienced more geopolitical change than any other financial crime discipline.
- Only **9%** reported effective real-time monitoring and interdiction controls.
- **50%** identified the alignment of global policy with local implementation as their greatest cross-jurisdiction challenge.

These are not abstract technology problems. They are operating challenges faced by the practitioners responsible for managing financial crime risk.

A sanctions match is a starting point, not a risk decision.

Modern sanctions programs need the ability to determine who an entity actually is, understand the ownership and relationships surrounding it, identify indirect exposure, and give analysts the evidence needed to act.

As you evaluate sanctions technology, look beyond how many lists a platform screens or how many alerts it can generate.

Ask a more important question:

Can it help us distinguish a potential match from actual risk?

Use the capabilities, evaluation criteria, proof-of-concept guidance, and RFP questions in this guide to put prospective vendors to the test.

Sources

Financial Action Task Force. *"Risk-Based Approach Guidance for the Banking Sector."* **FATF**

1LoD. *"Financial Crime Summit 2026 Research Report and Practitioner Findings on Sanctions, Geopolitical Risk, Real-Time Monitoring and Financial Crime Operating Models."* 2026. The practitioner-polling findings cited in this article appeared in the original source materials. Additional information about the participating financial crime and sanctions community is available from the **1LoD Financial Crime Summit.**

1LoD. *"Forecast 2026: One Financial Crime Risk With Many Channels."* April 15, 2026. **Read the report.**

1LoD Financial Crime Summit London. *"Interactive Roundtable Discussions: Continuous Client Risk Management and Sanctions Compliance."* 2026. **View the agenda.**

1LoD Financial Crime Summit New York. *"Understanding the Intersection of Trade Sanctions and Export Controls."* March 11, 2026. **View the session.**

U.S. Department of the Treasury, Office of Foreign Assets Control. *"A Framework for OFAC Compliance Commitments."* May 2, 2019. **Read the framework.**

The Wolfsberg Group. *"Guidance on Sanctions Screening."* Jan. 21, 2019. **Read the guidance.**

