

The Adverse Media & Reputational Risk Playbook.

Hear it first. **Act before it costs you.**

A practical guide to building an adverse media screening program: from regulatory expectations and risk appetite to data sources, false positives, workflows and board reporting.

CONTENTS

Twelve Chapters, Four Parts, One Reputational Risk Program

Introduction	3
--------------	---

PART 1 · THE NEW RISK LANDSCAPE

1	Why Adverse Media Matters More Than Ever	4
2	What Counts as Adverse Media?	8

PART 2 · BUILDING A MODERN ADVERSE MEDIA FRAMEWORK

3	Designing Your Risk-Based Approach	11
4	Data Sources and Coverage	14
5	Reducing False Positives Without Increasing Risk	16

PART 3 · OPERATIONALIZING ADVERSE MEDIA SCREENING

6	Workflow and Investigation Best Practices	18
7	Integrating Adverse Media into KYC/KYB	20
8	Board and Regulator Reporting	21

PART 4 · THE FUTURE OF REPUTATIONAL RISK

9	AI, Automation and Continuous Monitoring	23
10	The Compliance Checklist	25

CONCLUSION

11	Why sanctions.io Is Your Ideal Partner	28
12	Your Next Steps	29
	Sources	30

INTRODUCTION

The Rules of Compliance Have Changed

For years, the industry treated sanctions screening as a checkbox exercise: match a name against a list, document the result, and move on. **That approach is no longer sufficient.**

In a world of instant global communication, 24-hour news cycles and a proliferation of investigative journalism, a manual approach is no longer viable. The sheer volume and velocity of information mean that automated, continuously updated adverse media screening has become critical. A single negative headline can inflict more damage on an organization than a regulatory fine. Reputational risk has emerged as one of the most significant threats facing businesses today, and adverse media screening is the front line of defense.

This playbook is designed to be a practical, actionable guide for compliance professionals, risk managers and consultants, and business leaders who need to build or improve their adverse media screening programs. It covers the full lifecycle, from understanding the regulatory landscape and defining your risk appetite, to selecting the right data sources, reducing false positives, and reporting to the board.

Whether you are a fintech startup processing your first thousand customers or a global financial institution managing millions of relationships, the principles in this guide will help you **detect, assess, and manage reputational risk at scale.**

— PART 1 · THE NEW RISK LANDSCAPE · CHAPTER 1

Why Adverse Media Matters More Than Ever

The compliance landscape has undergone a seismic shift. Where organizations once focused primarily on reactive sanctions screening, the mandate has expanded to **proactive, holistic reputational risk management**.

Regulators, investors, and customers now expect firms to look beyond designated lists and identify potential risks hidden within a global torrent of publicly available information. This evolution from a reactive to a proactive stance is no longer a matter of best practice; it is a core requirement for survival and growth in the modern economy.

From reactive to proactive

The traditional compliance model was built around a simple premise: check a customer's name against a sanctions list, and if there is no match, proceed. This model was adequate in a world where information moved slowly and regulatory expectations were narrow. Today, however, the volume of publicly available information has exploded, and regulators expect firms to use it.

The shift is from a narrow focus on sanctions compliance to a broader mandate of reputational risk management. This means identifying potential risks before they crystallize into formal sanctions, enforcement actions, or full-blown scandals. Adverse media often surfaces before authorities catch wind of a case, providing a critical early warning signal.

Global regulatory expectations

Global regulatory bodies have been clear in their expectations. The Financial Action Task Force (FATF) has consistently emphasized a risk-based approach, which inherently requires firms to understand and vet the public and non-public profile of their clients and partners. The FATF's guidance on ongoing due diligence and enhanced monitoring explicitly lists adverse media screening as a best practice.¹

The European Union's Anti-Money Laundering Directives (AMLD), culminating in the comprehensive new AML Regulation (AMLR, Regulation (EU) 2024/1624), demand that firms assess publicly available information as part of their Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) obligations.²

In the United Kingdom, the Financial Conduct Authority (FCA) has explicitly stated that it expects firms to use adverse media screening during both onboarding and periodic reviews, citing failures to act on public information as a significant risk of facilitating money laundering.³ Across the Asia-Pacific region, the Monetary Authority of Singapore (MAS) and the Hong Kong Monetary Authority (HKMA) have both underlined the importance of adverse media screening, with HKMA identifying it as an "ideal candidate" for automation.⁴

The cost of missed negative media

The cost of failing to conduct adverse media screening is increasing and multi-faceted. Global fines for non-compliance reached \$14 billion in 2024, while AML, sanctions, and CDD penalties alone totaled \$3.8 billion in 2025.^{5,6} Non-compliant businesses spend an average of 2.7 times more on remediation than their compliant peers.⁷ These figures, however, only tell part of the story. The true cost extends to shattered brand trust, lost business, and diminished shareholder value, which can take years to rebuild.

\$14bnGLOBAL NON-COMPLIANCE
FINES, 2024**\$3.8bn**AML, SANCTIONS AND CDD
PENALTIES, 2025**2.7x**HIGHER REMEDIATION
SPEND WHEN NON-
COMPLIANT

Case studies of reputational fallout

Recent history is littered with cautionary tales. In each case, credible adverse media was available years before formal enforcement action was taken.⁸

Wirecard

2020 · Germany

The German fintech, valued at over €24 billion, collapsed after €1.9 billion in fabricated cash balances were exposed. Investigative reports from the Financial Times had been largely ignored, and the warning signs had been in the public domain since 2015.

Danske Bank

2007–2015 · Estonia

Over €200 billion in suspicious transactions flowed through the bank's Estonian branch. The scandal was foreshadowed by media reports and internal whistleblowers long before regulators intervened.⁹

1MDB

Malaysia

Billions were misappropriated from a Malaysian sovereign wealth fund, with global banks paying billions in penalties for their role in facilitating the scheme.

Volkswagen

2015 · “Dieselgate”

Diesel engines were programmed with a “defeat device” that detected emissions testing and adjusted performance to improve results. Over \$30 billion in fines and settlements followed, preceded by academic research and media reports that questioned the company's emissions data.

THE LESSON

Adverse media often provides the first, and sometimes only, warning of catastrophic risk. Ignoring these signals is no longer an option.

Negative news bias

It is also worth considering the concept of negative news bias. Research shows that negative news headlines attract significantly more attention than positive ones, and that readers are far more likely to engage with and share negative content.¹⁰ This means that the vast majority of the media landscape we are exposed to is inherently negative in tone.

For compliance professionals, this has a practical implication: the volume of potentially relevant adverse media is enormous, and without a structured, automated framework to filter and assess it, the risk of missing a genuine threat is high.¹¹

WHY IT MATTERS

Negative news is not the exception in the media landscape; it is the norm. A screening program has to be built for volume from day one.

PART 1 · THE NEW RISK LANDSCAPE · CHAPTER 2

What Counts as Adverse Media?

According to LSEG Risk Intelligence, adverse media is “any unfavourable information available about an individual, organisation, or entity, typically uncovered in media sources. These could range from allegations of financial crime, regulatory violations, or political corruption to criminal convictions.”¹²

It is not the same as a sanctions check, but rather a related risk-assessment process used to identify negative news, reports, or allegations about an individual or business, helping companies detect financial, legal, or reputational risks during KYC or AML checks.¹³ However, not all negative news carries the same weight. A modern adverse media framework requires a nuanced approach to categorizing and assessing this information to separate genuine threats from noise and false positives.

Crime vs. allegations vs. regulatory action

A fundamental distinction must be drawn between different types of adverse media. A confirmed criminal conviction carries a very different weight than an unproven allegation in a tabloid newspaper, which in turn is different from a formal regulatory investigation. Effective adverse media screening requires the ability to distinguish between these varying levels of threat, and between categories of risk (a fraud, a personal crime, and a money laundering story are not the same), and to assign an appropriate level of risk to each.

Importantly, regulators have made clear that adverse media does not need to prove wrongdoing to justify enhanced due diligence. An allegation from a credible source is sufficient to warrant further investigation.

Tiering severity: low, medium, and high-risk news

To manage this diverse information flow, leading compliance programs implement a risk-based tiering system. This allows analysts to prioritize alerts and focus on the most significant threats.

RISK TIER	DESCRIPTION AND EXAMPLES	TYPICAL ACTION
High	Confirmed links to financial crime, terrorism financing, sanctions evasion, or inclusion on a law enforcement most-wanted list.	Escalate immediately for senior review; consider offboarding.
Medium	Allegations of corruption, involvement in a significant regulatory investigation, or close association with a high-risk individual or entity.	Trigger Enhanced Due Diligence (EDD).
Low	Minor regulatory fines for non-systemic issues, negative consumer reviews, or uncorroborated allegations from non-credible sources.	Document and monitor; no immediate action required.

Politically exposed controversies

While being a Politically Exposed Person (PEP) is not inherently a risk, adverse media related to a PEP, such as allegations of corruption, abuse of power, or unexplained wealth, is a major red flag that requires immediate Enhanced Due Diligence. PEP-related adverse media is particularly significant because it often involves complex networks of associates and family members, making it essential to screen not just the individual but their entire sphere of influence.

ESG and human rights reporting

Environmental, Social, and Governance (ESG) issues represent a rapidly growing category of adverse media. Reports of environmental crimes, labor abuses, human rights violations, and poor corporate governance can lead to significant reputational damage and investor backlash. The Volkswagen emissions scandal is a prime example of how an ESG issue can escalate into a multi-billion-dollar crisis. As ESG reporting frameworks become more stringent and investor scrutiny intensifies, this category of adverse media will only become more important.

Social media vs. credible journalism

Finally, the credibility of the source is paramount. A report from an established international news organization, a court filing, or a regulatory notice carries far more weight than an anonymous blog post or an unverified social media post. While social media can sometimes provide early warnings, it must be corroborated by reputable sources before being factored into a formal risk assessment.

The ability to distinguish credible journalism from unsubstantiated claims is a cornerstone of an effective adverse media screening program. It is also important to distinguish between mainstream or international media and local or gazette media, as the latter may provide more granular, region-specific information that is not widely reported.

PART 2 · BUILDING A MODERN ADVERSE MEDIA FRAMEWORK · CHAPTER 3

Designing Your Risk-Based Approach

An effective adverse media screening program is not a one-size-fits-all solution. It must be tailored to an organization's specific risk profile, regulatory obligations, and business model. **This is the essence of the risk-based approach** advocated by the FATF and other global regulators.

It requires a thoughtful and deliberate process of defining what risk means to your organization and designing a framework that is both effective and proportionate.

Risk appetite definition

The first step is to define your risk appetite. This is a formal declaration of the level and type of risk your organization is willing to accept in pursuit of its business objectives. It should be approved at the board level and serve as the guiding principle for your entire compliance framework. For example, a fintech startup focused on rapid growth in emerging markets may have a different risk appetite than a centuries-old private bank serving ultra-high-net-worth individuals.

The risk appetite statement should explicitly address reputational risk and define which types of adverse media are unacceptable. Without a clear risk appetite, your compliance team will lack the direction needed to make consistent and defensible decisions. Key internal stakeholders such as the board of directors, senior management, and the compliance team should be involved in this decision, and external stakeholders like regulators and investors should also be considered.

Jurisdictional considerations

The regulatory requirements for adverse media screening can vary significantly from one country to another. A firm operating in the European Union must adhere to the stringent requirements of the AMLD and the new AMLR, which will be directly applicable from July 2027.¹⁴ A US-based firm will be guided by FinCEN's expectations and the Bank Secrecy Act. In the UK, the FCA's expectations are clear and well-documented. In the Asia-Pacific region, MAS, HKMA, and AUSTRAC all have their own specific guidance.

A global organization must create a framework that satisfies the strictest of these requirements, while also accounting for local nuances, such as data privacy laws (like GDPR) and the availability of reliable local-language media.

Customer risk tiering

With a clear risk appetite and understanding of jurisdictional requirements, you can implement customer risk tiering. This involves categorizing customers as low, medium, or high risk based on factors such as their industry, geography, products used, and entity type. This tiering directly informs the level of due diligence required. A low-risk customer might only require a basic adverse media check at onboarding, while a high-risk customer, such as a PEP from a high-risk jurisdiction, will require comprehensive, ongoing monitoring against a wide range of adverse media sources.

Onboarding checks vs. ongoing monitoring

This leads to the final core component of a risk-based approach: distinguishing between onboarding checks and ongoing monitoring. A one-time check at the beginning of a relationship is no longer sufficient. A customer's risk profile can change at any moment. A company director might be implicated in a bribery scandal, or a previously stable country might suddenly become a hotbed of political unrest.

Therefore, high-risk customers must be subject to continuous or periodic monitoring to ensure that any new adverse media is identified and assessed in a timely manner. This proactive approach is the only way to manage reputational risk effectively in a dynamic and unpredictable world.

AUTOMATE IT

The ability to automate ongoing monitoring is a critical capability, enabling compliance teams to receive real-time alerts when new adverse media emerges about a customer or counterparty, without the need for manual intervention.

PART 2 · BUILDING A MODERN ADVERSE MEDIA FRAMEWORK · CHAPTER 4

Data Sources and Coverage

A modern adverse media framework is **only as effective as the data that fuels it**. Relying on a simple web search is a recipe for disaster, as it provides no guarantee of comprehensive coverage, source credibility, or auditability.

A robust data strategy must be multi-layered, incorporating a wide range of sources to create a complete and accurate picture of a counterparty's risk profile.

Global news sources

The foundation of any adverse media screening program is global news sources. This includes major international publications such as Reuters, the Financial Times, and the Associated Press, as well as national newspapers and reputable online news outlets. These sources provide broad coverage of major events and are often the first to report on significant allegations of wrongdoing.

Local language coverage

However, relying solely on global, English-language sources can create dangerous blind spots. Local language coverage is essential for identifying risks that may not be significant enough to make international headlines but are well-known within a specific country or region. A local corruption scandal or regulatory fine might only be reported in the local language, making it invisible to an English-only screening process. A comprehensive screening solution must be able to ingest and analyze content in multiple languages and scripts.

Structured vs. unstructured data

Structured data is neatly organized and easy to search, such as official sanctions lists, criminal watchlists, and PEP databases. This data is critical for identifying known high-risk individuals and entities. However, the vast majority of adverse media exists as unstructured data: the messy, unorganized world of news articles, blog posts, court filings, and social media. This is where the real challenge, and opportunity, lies. Unstructured data provides the context, nuance, and early warning signs that structured lists often lack.

Sanctions lists vs. media feeds

Sanctions lists are definitive; if a person or entity is on a list, you are restricted in doing business with them. Media feeds, on the other hand, are often indicative, although they sometimes state facts such as a confirmed prosecution. They provide information that must be assessed and interpreted. An allegation in a newspaper is not the same as a formal designation by a government body. A robust framework must be able to process both types of information and apply the appropriate level of scrutiny to each.

AI and NLP in media screening

This is where Artificial Intelligence (AI) and Natural Language Processing (NLP) become indispensable. Manually sifting through thousands of news articles in multiple languages is an impossible task. AI-powered platforms can automate this process, using NLP to understand the context of an article, identify the specific individuals and entities involved, and categorize the type of risk being reported.¹⁵ This technology allows compliance teams to move beyond simple keyword matching and conduct sophisticated, context-aware screening at scale. Without AI, a truly global and comprehensive adverse media screening program is simply not feasible. Automation can also support ongoing monitoring and real-time risk assessment.

PART 2 · BUILDING A MODERN ADVERSE MEDIA FRAMEWORK · CHAPTER 5

Reducing False Positives Without Increasing Risk

One of the greatest operational challenges in adverse media screening is managing the high volume of false positives. Legacy screening systems that rely on simple keyword matching can generate a flood of irrelevant alerts, with some industry reports citing **false positive rates as high as 90 to 95%.**¹⁵

This “alert fatigue” not only wastes valuable analyst time but also increases the risk that a genuine threat will be missed amidst the noise. The goal of a modern framework is not simply to reduce false positives, but to do so intelligently, without inadvertently increasing risk. Robust data from a provider with smart matching capabilities and automated ongoing monitoring is one way to achieve this.

Name-matching logic

Simple string matching is no longer sufficient. Modern screening engines use sophisticated algorithms that can account for transliteration issues (e.g., Mohammed, Mohamed, Muhammad), nicknames, aliases, and cultural naming conventions, as well as variations across scripts such as Jawi, Latin and Hanzi. This ensures that the system can identify relevant individuals even when their names are spelled differently across various sources, while simultaneously filtering out irrelevant matches.

Context extraction

A name alone is meaningless without context. Advanced systems use NLP to analyze the content of an article and determine whether the person mentioned is the subject of the adverse media or merely a passing reference. For example, an article might mention a “John Smith” who is a witness to a crime, not the perpetrator. NLP can distinguish between these scenarios, preventing an irrelevant alert from being generated.

Negative keyword logic

This involves using specific keywords to exclude irrelevant results. For example, if you are screening for financial crime, you might use negative keywords like “actor,” “film,” or “movie” to filter out articles about a celebrity with the same name as your client. This simple but effective technique can significantly reduce the number of false positives from entertainment or sports news.

Entity resolution

This is the process of determining whether multiple records in different data sources refer to the same real-world entity. An effective screening platform can consolidate information from various sources, such as news articles, corporate registries, and social media, to create a single, unified profile of an individual or company. This provides a more complete picture of risk and helps to eliminate duplicate or conflicting alerts.

Human review workflows

Technology alone is not enough. A well-defined workflow for human review is essential for handling the complex cases that automated systems cannot resolve. This should include a clear process for escalating high-risk alerts, documenting investigation findings, and providing feedback to the system to improve its accuracy over time. This human-in-the-loop approach ensures that the system is constantly learning and adapting, leading to a continuous reduction in false positives without compromising the integrity of the screening process.

One highly effective way to design and document these workflows is through Business Process Model and Notation (BPMN), a standardized graphical notation that allows compliance teams to map out complex human review workflows in a clear and universally understood format.

PART 3 · OPERATIONALIZING ADVERSE MEDIA SCREENING · CHAPTER 6

Workflow and Investigation Best Practices

An effective adverse media screening program is built on a foundation of **clear, consistent, and auditable workflows**. Without a structured process for managing alerts, even the most advanced technology can fail.

Best practices in this area focus on creating a systematic approach to alert triage, investigation, and escalation that ensures both efficiency and accountability.

Alert triage frameworks

At the heart of this process is an alert triage framework. This is a set of rules that governs how incoming alerts are prioritized and assigned. Not all alerts are created equal, and analysts should not be expected to treat them as such. A well-designed triage framework will automatically categorize alerts based on the risk tiering system defined in your risk-based approach. High-risk alerts, such as a direct match to a known financial criminal, should be flagged for immediate review, while low-risk alerts can be queued for later analysis or even automatically dismissed if they fall below a certain materiality threshold.

Escalation matrices

Once an alert has been triaged and investigated, all activities must be governed by clear escalation matrices. These are predefined pathways that dictate when and to whom an alert should be escalated. For example, an alert that is confirmed as a true match to a high-risk individual might be automatically escalated to a senior compliance officer or a dedicated risk committee.

A TYPICAL ESCALATION MATRIX

SEVERITY	INVESTIGATED BY	ESCALATED TO	TIMELINE
High	Senior Analyst	MLRO / Risk Committee	Within 4 hours
Medium	Analyst	Senior Analyst / Team Lead	Within 24 hours
Low	Junior Analyst / Automated	Analyst (if flagged)	Within 5 business days

This removes ambiguity from the process and ensures that critical decisions are made by the appropriate personnel within a defined timeframe.

Documentation standards and audit trails

Every step of the workflow must be meticulously documented. Documentation standards should be established to ensure that all investigation findings, decisions, and rationale are recorded in a consistent and auditable format. This creates a clear audit trail that can be used to demonstrate to regulators that a thorough and risk-based approach was taken.

Key elements to document include the date and time of the alert, the source of the adverse media, the investigation steps taken, the analyst's assessment, and the final decision and rationale. In the event of a regulatory inquiry, the ability to produce a complete and well-documented case file can be the difference between a clean bill of health and a significant enforcement action.

REMOVE THE BURDEN

Many screening and monitoring providers, like sanctions.io, create automatic audit trails so that documentation does not depend on manual effort.

PART 3 · OPERATIONALIZING ADVERSE MEDIA SCREENING · CHAPTER 7

Integrating Adverse Media into KYC/KYB

Adverse media screening should not be a standalone process. To be truly effective, it must be deeply integrated into your organization's core Know Your Customer (KYC), Know Your Business (KYB) and Anti-Money Laundering (AML) workflows.

This integration ensures that reputational risk is considered at every stage of the customer lifecycle, from initial onboarding to ongoing monitoring.

Individual onboarding

For individual onboarding, adverse media checks should be conducted in parallel with sanctions screening. This provides a more complete picture of the individual's risk profile from the outset. For example, a new customer might clear all sanctions lists but have a history of being publicly associated with fraudulent schemes. This information, which would only be revealed through an adverse media check, would be a critical factor in determining whether to accept the customer or subject them to enhanced due diligence.

Ongoing monitoring

Integration is not a one-time event. Ongoing monitoring is essential for managing risk throughout the customer relationship. A customer's risk profile is not static; it can change at any time. A key executive might be indicted, a company might be implicated in an environmental disaster, or a previously stable country might descend into political turmoil. An integrated system will automatically trigger a review when new adverse media is detected for an existing customer, allowing the compliance team to reassess the relationship and take appropriate action.

This continuous feedback loop between adverse media screening and the core KYC/KYB platform is the hallmark of a mature and effective compliance program.

PART 3 · OPERATIONALIZING ADVERSE MEDIA SCREENING · CHAPTER 8

Board and Regulator Reporting

An adverse media screening program does not operate in a vacuum. Its insights and outcomes must be communicated effectively to both internal and external stakeholders, including the board of directors and regulators.

This reporting is not merely an administrative task; it is a critical function that demonstrates the effectiveness of your compliance program and provides assurance that reputational risk is being managed proactively.

For the board, reporting should focus on high-level trends and key performance indicators (KPIs). The board is not interested in the details of every individual alert, but they do need to understand the overall health of the program and the nature of the risks the organization is facing.

KPI	WHAT IT MEASURES	WHY IT MATTERS
Alert volume and trends	Total alerts generated, broken down by risk tier and geography.	Identifies emerging risk hotspots and trends.
True positive rate	Percentage of alerts confirmed as genuine risks.	Demonstrates the efficiency and accuracy of the screening engine.
False positive rate	Percentage of alerts dismissed as irrelevant.	Highlights opportunities to optimize screening rules.
Time to resolution	Average time to investigate and close an alert.	Key measure of operational efficiency and resource allocation.
High-risk escalations	Number of alerts escalated to senior management or risk committee.	Provides visibility into the most significant threats.
Ongoing monitoring coverage	Percentage of high-risk customers under continuous monitoring.	Measures the maturity and comprehensiveness of the program.

Risk dashboards

This information is often best presented in the form of risk dashboards. A well-designed dashboard can provide an at-a-glance view of the program's performance and highlight any areas that require attention. Visualizations such as heat maps showing the geographic distribution of risk, or trend lines showing the evolution of alert volumes over time, can be particularly effective for communicating complex information to a non-specialist audience.

Demonstrating proportionality

When it comes to reporting to regulators, the focus shifts from high-level trends to demonstrating the robustness and proportionality of your program. Regulators want to see that you have a well-documented, risk-based approach and that you are applying it consistently. This requires the ability to produce detailed audit trails for any given customer, showing when they were screened, what was found, and how many alerts were investigated and resolved.

You must be able to explain why a particular customer was assigned a certain risk rating and why the level of due diligence applied was appropriate for that level of risk. This is where the meticulous documentation standards discussed earlier become invaluable.

IN AN EXAMINATION

A clear and comprehensive paper trail is your best defense.

PART 4 · THE FUTURE OF REPUTATIONAL RISK · CHAPTER 9

AI, Automation and Continuous Monitoring

The future of adverse media screening is being defined by the convergence of artificial intelligence, automation, and continuous monitoring. The sheer volume and velocity of global information have **made manual screening processes obsolete**.

Organizations that fail to embrace these technological advancements will find themselves unable to keep pace with the evolving risk landscape and the expectations of regulators. For a deeper dive into how automation is reshaping the compliance function as a whole, see the sanctions.io guide **The Future of Compliance Automation**.

Real-time alerts

The most immediate benefit of modern screening technology is the ability to generate real-time alerts. In a world where a news story can break at any moment, the ability to be notified instantly when a customer or counterparty is mentioned in adverse media is invaluable. This allows compliance teams to be proactive, not reactive, in their risk management. For example, if a key executive at a client company is suddenly implicated in a corruption scandal, a real-time alert allows you to immediately reassess the relationship and take appropriate action, rather than discovering the information weeks or months later during a periodic review.

Predictive risk indicators

The combination of AI and continuous monitoring can enable the identification of predictive risk indicators. By analyzing vast datasets of historical information, AI models can identify patterns and correlations that may signal future risk. For example, a sudden increase in negative media coverage around a particular industry or region could be an early indicator of emerging geopolitical or regulatory risk. A cluster of seemingly unrelated adverse media reports about different entities within the same corporate group could signal a systemic issue. These predictive capabilities represent the next frontier in reputational risk management.

Automation vs. human judgment

However, it is crucial to remember that technology is a tool, not a panacea. The future of reputational risk management will not be about replacing human judgment, but about augmenting it. AI excels at processing vast quantities of data, identifying patterns, and flagging potential risks. But the final decision on how to respond to an alert, whether to escalate or whether to offboard a customer, requires the nuanced judgment of a trained compliance professional.

The most effective compliance programs will be those that find the optimal balance between automation and human expertise, using technology to handle the scale and complexity of the data, while relying on skilled analysts to make the final, nuanced risk decisions.

MCKINSEY ON AGENTIC AI

Agentic AI can complete analytical tasks faster and more efficiently than humans, with prominent use cases including false positive detection in AML screening. Human oversight, however, remains essential.¹⁶

PART 4 · THE FUTURE OF REPUTATIONAL RISK · CHAPTER 10

The Compliance Checklist

The demands on compliance teams will only continue to grow. The regulatory landscape is in constant flux, and the technologies used by both legitimate and illicit actors are evolving at a breakneck pace. To stay ahead of the curve, organizations must be **proactive in assessing their capabilities** and developing a clear roadmap for the future.

Implementation roadmap

A successful implementation is a journey, not a destination. It requires a phased approach that builds a solid foundation before moving on to more advanced capabilities.

PHASE	TIMELINE	KEY ACTIVITIES
1: Foundation	First 3 months	Define and document your risk appetite. Conduct a comprehensive risk assessment of your customer base. Select and implement an AI-powered adverse media screening solution. Develop and document your core triage and investigation workflows.
2: Integration	Months 3–6	Integrate your adverse media screening solution with your core KYC/KYB platform. Automate the screening of all new customers at onboarding. Begin periodic screening of your high-risk customer segment.
3: Optimization	Months 6–12	Implement continuous monitoring for all high-risk customers. Develop and roll out board-level risk dashboards and KPIs. Conduct a full review of your false positive rates and refine your screening rules accordingly.
4: Maturity	Beyond 12 months	Expand continuous monitoring to your medium-risk customer segment. Explore the use of predictive risk indicators. Conduct regular, independent audits of your program to ensure its ongoing effectiveness.

Maturity model

Where does your organization stand today? Use this maturity model to assess your current capabilities and identify areas for improvement.

LEVEL	DESCRIPTION
1: Basic	Screening is manual, ad hoc, and relies on basic web searches. There is no formal risk appetite or documented workflow.
2: Developing	A third-party screening tool is in use, but it relies on simple keyword matching. False positive rates are high, and the process is largely manual.
3: Established	An AI-powered screening solution is in place, and workflows are documented. Screening is integrated into onboarding, and high-risk customers are subject to periodic review.
4: Advanced	Screening is fully automated and integrated across the customer lifecycle. Continuous monitoring is in place for high-risk customers, and KPIs are reported to the board.
5: Leading	The program is predictive, not just reactive. AI is used to identify emerging risks, and the compliance function is seen as a strategic partner to the business, enabling safe and sustainable growth.

Self-assessment scorecard

Rate your organization on a scale of 1 to 5 (1 = not at all, 5 = fully implemented) for each of the following capabilities.

#	CAPABILITY	RATING (1-5)
1	A board-approved risk appetite for reputational risk is in place.	<input type="text" value="1"/> <input type="text" value="2"/> <input type="text" value="3"/> <input type="text" value="4"/> <input type="text" value="5"/>
2	We have a documented, risk-based approach to adverse media screening.	<input type="text" value="1"/> <input type="text" value="2"/> <input type="text" value="3"/> <input type="text" value="4"/> <input type="text" value="5"/>
3	Our screening process includes local language and unstructured data sources.	<input type="text" value="1"/> <input type="text" value="2"/> <input type="text" value="3"/> <input type="text" value="4"/> <input type="text" value="5"/>
4	We use an AI-powered solution to reduce false positives and extract context.	<input type="text" value="1"/> <input type="text" value="2"/> <input type="text" value="3"/> <input type="text" value="4"/> <input type="text" value="5"/>
5	Adverse media screening is fully integrated into our KYC/KYB workflows.	<input type="text" value="1"/> <input type="text" value="2"/> <input type="text" value="3"/> <input type="text" value="4"/> <input type="text" value="5"/>
6	We have a clear and auditable workflow for alert triage and investigation.	<input type="text" value="1"/> <input type="text" value="2"/> <input type="text" value="3"/> <input type="text" value="4"/> <input type="text" value="5"/>
7	We conduct continuous or periodic monitoring of our high-risk customers.	<input type="text" value="1"/> <input type="text" value="2"/> <input type="text" value="3"/> <input type="text" value="4"/> <input type="text" value="5"/>
8	We report on adverse media KPIs to the board and senior management.	<input type="text" value="1"/> <input type="text" value="2"/> <input type="text" value="3"/> <input type="text" value="4"/> <input type="text" value="5"/>
9	Our compliance team has the skills and resources to manage a modern screening program.	<input type="text" value="1"/> <input type="text" value="2"/> <input type="text" value="3"/> <input type="text" value="4"/> <input type="text" value="5"/>
10	We view our compliance program as a strategic enabler of growth.	<input type="text" value="1"/> <input type="text" value="2"/> <input type="text" value="3"/> <input type="text" value="4"/> <input type="text" value="5"/>

SCORING

40 to 50 = Leading · 30 to 39 = Advanced · 20 to 29 = Established · 10 to 19 = Developing · Below 10 = Basic

Use this score to identify your position on the maturity model and prioritize your next steps.

CONCLUSION · CHAPTER 11

Why sanctions.io Is Your Ideal Partner

Building a best-in-class adverse media screening program requires the right technology partner. sanctions.io provides a comprehensive, AI-powered screening platform that is **trusted by 400+ organizations worldwide**, from fast-growing fintechs to established financial institutions.

Comprehensive data coverage

sanctions.io provides access to over 100 data sources, including 80+ sanctions and watchlists from 30+ jurisdictions, PEP databases, criminal watchlists, and adverse media feeds. Data is cleansed, standardized, and enriched, with sanctions lists updated every 60 minutes, ensuring you always have the latest information at your fingertips.

AI-powered smart matching

The platform's name-matching technology leverages the latest research in NLP and Machine Learning to overcome real-world challenges in screening, including transliteration issues, nicknames, spelling errors, and honorifics. This significantly reduces false positives while ensuring that no real matches slip through the cracks.

Flexible solutions for any workflow

Whether you need a real-time screening API with an average response time of approximately 350 milliseconds, a batch screening API for processing thousands of entities simultaneously, a manual screening portal, or continuous monitoring with real-time alerts, sanctions.io has a solution that fits your needs. Pre-built integrations for SAP, BigID, Salesforce, and HubSpot make it easy to embed screening into your existing workflows.

Enterprise-grade reliability

With a system uptime of 99.995% and SOC 2 compliance, sanctions.io provides the reliability and security that enterprise compliance teams demand. Auditable timestamps ensure you are always ready for auditors and regulators.

Transparent pricing

Unlike many competitors, sanctions.io offers transparent, volume-based pricing that allows you to calculate your costs upfront. There are no hidden fees or surprises. Use our **Transparent Pricing Calculator** to get an instant estimate based on your business needs.

— CONCLUSION · CHAPTER 12

Your Next Steps

- 1** Assess your current state. Use the self-assessment scorecard in Chapter 10 to evaluate your organization's current adverse media screening capabilities and identify your position on the maturity model.
 - 2** Explore our **Unified Guide to Screening** and learn how to combine adverse media screening with sanctions and PEP screening for a comprehensive, streamlined compliance workflow. Deepen your knowledge of sanctions, compliance and AML screening using our resources at **sanctions.io/resources**.
 - 3** Use our **Risk Calculator** to audit your exposure against sanctions and other watchlists, and find out which watchlists your organization is required to screen against.
 - 4** Ready to take the next step? **Book a call** with our experts and receive a free 7-day trial (no credit card required). Take the time to discuss your specific needs and learn how we can help you build a world-class AML and adverse media screening program.
-

Talk to an expert

Prefer to talk it through? See how your compliance process can go from inefficient to simple, scalable and unified.

"The product is amazing and the tech is tight. We integrated the sanctions.io API within a couple of days and now perform daily screenings of our entire customer base."

Dan Westgarth, COO, Deel Inc.

REFERENCES

Sources

-
- 1 **Financial Action Task Force (FATF), The FATF Recommendations (2024)**
fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

 - 2 **European Parliament and Council, Regulation (EU) 2024/1624 on the prevention of the use of the financial system for money laundering or terrorist financing (AMLR) (2024)**
eur-lex.europa.eu/eli/reg/2024/1624/oj

 - 3 **Financial Conduct Authority, Dear CEO Letter: Common control failings identified in anti-money laundering frameworks (2021)**
fca.org.uk/publications/correspondence

 - 4 **Hong Kong Monetary Authority, AML/CFT Regtech: Case Studies and Insights (2021)**
hkma.gov.hk/eng/key-functions/banking/anti-money-laundering-and-counter-financing-of-terrorism/regtech

 - 5 **StarCompliance, The Global Cost of Non-Compliance in 2024 (2024)**
starcompliance.com

 - 6 **Fenergo, Global financial regulatory penalties fall by 18% in 2025 as enforcement shifts from US to EMEA and APAC (2025)**
fenergo.com

 - 7 **PayCompliance, The Cost of Non-Compliance: Financial and Reputational Risks for Businesses (2025)**
paycompliance.com

 - 8 **sanctions.io, The Cost of Failed Adverse Media Checks (2026)**
sanctions.io/blog
-

-
- 9 **sanctions.io, What Is Adverse Media Screening? (Danske Bank case study) (2025)**
sanctions.io/blog
-
- 10 **ResearchGate, Negative news headlines are more attractive: negativity bias in online news reading and sharing (2023)**
researchgate.net
-
- 11 **PMC, Is Bad News More Likely to Be Published? (2024)**
pmc.ncbi.nlm.nih.gov
-
- 12 **LSEG Risk Intelligence, Adverse Media in Risk Management**
lseg.com/en/risk-intelligence
-
- 13 **Projective Group, EU Anti-Money Laundering Framework Alert: Requirements for Customer Due Diligence to Become More Comprehensive (2025)**
projectivegroup.com
-
- 14 **sanctions.io, The Role of AI in Sanctions and PEP Screening (2025)**
sanctions.io/blog
-
- 15 **McKinsey & Company, The investigator-centered approach to financial crime: Doing what matters (2020)**
mckinsey.com/capabilities/risk-and-resilience/our-insights
-
- 16 **McKinsey & Company, How agentic AI can change the way banks fight financial crime (2025)**
mckinsey.com/capabilities/risk-and-resilience/our-insights
-