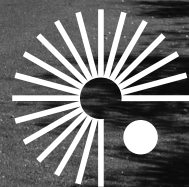


Compliance: A Data-Driven Playbook

In a world brimming with uncertainty,
proactive compliance is an absolute must.



opoint



Table of Contents

- **Executive Summary**
- **Trends Shaping Compliance**
- **AML, KYC, and Perpetual Monitoring**
- **Alert Overload**
- **The Non-English Advantage**
- **Building a Strong Compliance Foundation**
- **Actionable Steps**
- **Expert Q&A: Insights from Toby Cook, CSO @ Opoint**
- **Lessons from Real-World Compliance Failures**
- **How Opoint Helps You Stay Compliant**
- **Future-Proof Your Compliance Strategy**
- **Key Takeaways**



Executive Summary

Why it Matters

We all know compliance isn't just about ticking a box—it's about ensuring compliance with diverse regulations while guarding against data breaches and reputational harm.

In 2025, businesses operate in a climate of heightened regulatory scrutiny and expanding technological capabilities, like machine learning and real-time data analytics. Core to this evolution is the rise of adverse media screening, which helps organisations spot emerging red flags in global news before they blow up into major scandals.



In an increasingly fractured regulatory environment, the onus is on compliance teams to cover as much of the threat landscape as possible.

Simply put, if you're a financial institution or business required to screen entities before engaging with them, can you really afford to miss critical information developing in the news?

James Hannan,
Risk Specialist @ Opoint

Who Should Read This?

If you're a Compliance Officer, Risk Manager, or Legal Advisor, this guide is written for you. It addresses your day-to-day pain points—managing overwhelming data streams, monitoring third-party risks, and staying ahead of regulatory changes.

We explore how to safeguard sensitive data and tap into real-time news (including non-English sources) that others might overlook, so you can catch adverse events the minute they surface.



Trends Shaping Compliance

As a compliance professional, your job is getting more complex. Every regulatory update, technological advance, or shift in monitoring practices directly impacts your workload, stress levels, and available resources.

Staying ahead means knowing what is changing and clearly understanding how these trends affect your daily responsibilities and long-term strategic planning. The key trends outlined below will shape your compliance landscape, influencing how you manage risks, allocate resources, and safeguard your organisation's reputation.

Consolidation of Regulations

Bodies like the Financial Action Task Force ([FATF](#)) want to ensure information security management across the financial sector. The EU and the US are rolling out stricter compliance strategies, focusing on beneficial ownership transparency and data integrity checks.



Technology Takes Centre Stage

Data analysis, real-time alerts, machine learning, and adverse media screening are game-changers in detecting suspicious activities.

Perpetual Monitoring vs Periodic Screening

Regulators increasingly favour continuous data processing to catch risks in near real-time. If you rely solely on periodic checks, you could miss crucial signals.





Cautionary Tales

Major enforcement actions in recent years highlight what happens when compliance processes fail to meet these evolving expectations. Regulators are levying more significant fines than ever and making enforcement very public, turning failures into headline news.

For those in compliance, these incidents serve as stark warnings of the stakes involved:

- **Danske Bank Scandal:** Danske Bank's money-laundering scandal revealed how failing to manage cross-border data effectively can enable illicit flows on a massive scale. Between 2007 and 2015, an estimated €200 billion in suspicious transactions were funnelled through its Estonian branch.

The fallout – criminal investigations, resignations, and enduring reputational damage – underscores how a lapse in oversight can become one of the largest money laundering cases in history. Enforcement actions also came with intense media scrutiny, amplifying the damage for the bank caught off guard.



Negative news is repeatedly linked to reputational risk and prolonged damage to business operations. Yet, many companies still treat adverse media screening as an afterthought.

In today's environment, failing to monitor emerging risks can be just as dangerous as failing to act.

James Hannan,
Risk Specialist @ Opoint



AML, KYC, and Perpetual Monitoring

One of the daily dilemmas for compliance teams is how to allocate resources between upfront due diligence (AML/KYC at onboarding) and ongoing monitoring. Both are critical, but they serve different purposes.

Perpetual Monitoring vs Periodic Screening

Onboarding checks

Scheduled compliance checks at set intervals. Think of it like your routine medical check-up.

Strengths:

- Good for stable, low-risk scenarios.
- Lower upfront costs.
- Familiar to regulators.

Limitations:

- Risks may go unnoticed between intervals.
- Potential delays in detecting emerging threats.
- May lead to compliance blind spots.

Perpetual Monitoring

Continuous real-time monitoring. It acts like a 24/7 security camera, always alert and vigilant.

Strengths:

- Immediate detection of emerging risks.
- Reduced risk of missing critical events.
- Ideal for dynamic, fast-paced environments.

Limitations:

- Higher initial investment.
- Requires proper integration and automated filtering to avoid alert fatigue.

Which One Is Right for You?

- Periodic Screening fits when risks are predictable and evolve slowly.
- Perpetual Monitoring excels in environments where immediate awareness is critical and risks are continuously evolving.
- Hybrid approaches are often optimal—combining periodic checks for routine compliance with perpetual monitoring for higher-risk scenarios.



The Case for Real-Time Data

In the era of instant information, real-time data analytics have become a lifeline for compliance professionals.

Strategic benefits include:

Stay a Step Ahead



Real-time analytics let you spot anomalies the moment they appear, rather than waiting for the following scheduled review. Early detection means early intervention – potentially preventing a minor issue from becoming a major violation.

Proactive Compliance



You minimise potential fines and reputational harm by catching negative news or suspicious transactions early. It's the difference between reading about your business in tomorrow's scandal headlines versus addressing a problem quietly today.

Reduced Manual Work



High-quality, machine learning-powered solutions can sift through thousands of sources and transactions in seconds. This cuts down the drudgery of manual data triage. Your analysts aren't spending their days scrolling through irrelevant alerts; instead, they can focus on the genuine red flags that genuinely need human judgment.



Spotlight on Data Integrity

With great volumes of data comes great responsibility – and new challenges. Compliance teams must ensure that the data fueling their decisions is accurate, secure, and actionable:

False Positives

Poor-quality or incomplete data can trigger a flood of false alerts, burying the real threats. Fine-tuning your data inputs (and using intelligent filtering) is key to avoiding “alert fatigue.” Otherwise, compliance officers can drown in noise and possibly miss the needle in the haystack.



Data Security



As compliance systems integrate more data (including personal and sensitive information from customers and third parties), protecting that data becomes paramount. A breach isn't just an IT issue, it's a compliance failure, too. Ensuring strong data encryption, access controls, and vendor security due diligence is now part of the compliance officer's remit.

Alert Overload

More data streams and monitoring tools can ironically lead to information overload. Without proper filters and risk scoring, you risk drowning in low-priority alerts while a critical issue hides in the clutter. Setting the proper parameters and continuously tuning your systems is a daily task to keep the signal-to-noise ratio healthy.





The Non-English Advantage

In today's globalised economy, risk knows no language boundaries. Yet many compliance programs remain too Anglo-centric, monitoring only English-language sources. This can be a costly blind spot.

Relying on English-only sources could mean missing vital stories that break first in Arabic, Chinese, Spanish, or any of the world's other major languages. Monitoring local-language news and data streams ensures you're not blindsided by regional events that later become international scandals.

- **Early-Bird Insights:** A local newspaper in Eastern Europe or Latin America might flag a money laundering scheme or corruption scandal days before it reaches the English press. Suppose you're tapped into those local sources. In that case, you gain precious lead time to investigate or mitigate the issue before it explodes globally.
- **Competitive Edge:** If your peers or competitors only watch English sources, a robust multi-language adverse media screening program will help you catch threats (or opportunities) before they do. Being the first to know can significantly prevent financial crime or avoid a bad business partner.

Simply put, the majority of the world's information is not in English. Compliance teams that recognise this and broaden their scope can catch risks others miss.



[Visit Our Global Coverage Map](#)



Practical Integration of Non-English News

Incorporating non-English content into your compliance workflow may sound daunting, but modern tools make it quite feasible:



Automated Translation

Today's AI translation tools instantly convert non-English news content into your chosen language.

Your team quickly grasps emerging stories—no waiting needed.

Custom Alerts & Filters

Configure data feeds by language, region, or keywords to receive only relevant alerts.

Use corporate identifiers (LEIs, stock tickers) to match foreign news directly to your monitored entities.



Layer with Machine Learning

Machine learning algorithms detect patterns or keywords in multiple languages, flagging unusual activity or sentiment immediately.

Gain deeper insights without overwhelming your team.

Global coverage introduces more data, but smart filtering and translation make it an attainable and hugely beneficial expansion of your compliance surveillance.



Building a Strong Compliance Foundation

Every business has a unique risk profile, so a one-size-fits-all compliance plan won't cut it. However, certain core steps add value to nearly any compliance program.

The following action plan is designed to strengthen your foundation, making daily operations more efficient and aligned with best practices.



Every business is unique, and so are its compliance needs. If enhanced due diligence is required, especially across multiple jurisdictions, adverse media screening and real-time insights become non-negotiable.

James Hannan,
Risk Specialist @ Opoint





1

Assess Your Current Compliance Strategy

Gap Analysis:

Evaluate how you conduct adverse media screening and update customer due diligence. Identify if you're only screening at onboarding, missing ongoing monitoring, or experiencing delays in flagging news.

Regulatory Scan:

Regularly review new mandates on data security, privacy, and reporting. Subscribe to newsletters or use update services to ensure no rule change affects your program.

2

Adopt or Enhance Perpetual Monitoring

Automation:

Implement tools that monitor transactions and news 24/7, automatically alerting your team to anomalies—eliminating the need for manual reviews.

Adverse Media Alerts:

Ensure your system flags negative news (including non-English sources) as soon as it appears, allowing early risk management.

Seamless Integration:

Integrate these tools into your existing workflows (CRM, case management, etc.) so alerts are managed within your regular processes.

3

Leverage Structured Data

Metadata Matters:

Tag articles and reports with metadata (e.g., company names, risk categories, dates, sources, languages) to enable fast filtering and searching.

Machine-Readable Formats:

Use XML or JSON feeds to allow automated parsing, reducing manual workload and speeding up analysis.



4

Integrate Non-English Coverage

Global Reach:

Expand monitoring beyond English sources—include local outlets from regions relevant to your operations (e.g. Middle East, East Asia).

Cross-Referencing:

Verify critical information by comparing multiple sources, ensuring the data's accuracy and integrity.

5

Stay Abreast of Regulatory Updates

Automated Feeds:

Subscribe to official bulletins (FATF, European Commission, FinCEN, etc.) to receive timely updates on new guidance and enforcement actions.

Leverage Platforms:

Use compliance software that integrates real-time policy change alerts, helping you adjust protocols seamlessly.

6

Train Your Teams

Ongoing Education:

Establish a regular training schedule (e.g., quarterly workshops, annual refreshers) to keep your team updated on regulations and best practices.

Cross-Functional Collaboration:

Foster cooperation between compliance, IT, risk management, and vendor teams to ensure everyone understands the importance of due diligence and data security.



Expert Q&A: Insights from Toby Cook, CSO @ Opoint

To get a practical perspective on these challenges, we spoke with [Toby Cook](#), Chief Sales Officer at Opoint, who has extensive experience in compliance data solutions. He offers insights into what compliance teams are facing now and how to prepare for the future.



From your perspective, what are the biggest compliance challenges organisations will face in 2025, and why should they start preparing now?



One of the biggest compliance challenges I foresee is the increasing demand for thorough [Adverse Media screening](#). Too often, companies do the bare minimum—treating screening like a check-box exercise.

As regulation tightens, simply skimming headlines won't cut it. Organisations need a comprehensive approach to spot early warnings in global media, not just the mainstream outlets. Starting now means you can build robust processes, integrate better data sources, and ultimately avoid nasty surprises down the road.



We've seen a growing shift from onboarding checks to continuous or perpetual monitoring. What are the key benefits of a real-time approach, and how can businesses transition smoothly?



Periodic checks can catch issues at the outset, but what happens three, six, or nine months later? If you're not monitoring continuously, risk can slip through undetected. Perpetual monitoring ensures you're alerted the moment suspicious activity emerges — even if a client looked spotless on day one.

From both a regulatory and a business standpoint, that real-time awareness is invaluable. For a smooth transition, start by reviewing your current onboarding processes and identify which elements could run continuously. Then, integrate tools that automate those checks.

As the old cliché tells us, if a job's worth doing, it's worth doing well.



Adverse media screening is often cited as a critical step in uncovering potential risks. Can you share strategies or best practices for implementing effective adverse media screening in a global, multilingual environment?



The biggest difference between adverse media screening and regular media monitoring is the need for global local content. It's amazing how many critical issues are picked up in local media and never make it to mainstream western press, or only make it there once the proverbial has already hit the fan!

If you just want to keep up to date with global issues, one of the big international news brands is fine. But if you are doing serious adverse media screening, those are much less valuable compared to truly global aggregation of local news. Very often, that also means screening non-English content.



Many organisations overlook local-language news, which often reports major scandals before they reach mainstream English outlets. How can compliance teams incorporate non-English sources into their workflows without overwhelming their data processing?



That's a difficult balancing act, but global organisations need to get their heads around the fact that the majority of the world's media is not written in English.

Take the Opoint feed as an example. We have more English-language content than anyone else, but it still only makes up about 40% of our total coverage.

In 2025, there is no way to avoid the need to become expert in screening content from non-English sources. The Opoint feed is normalised and delivered in XML or JSON, making translation relatively straightforward.



We're hearing a lot about the use of AI and machine learning in compliance, especially for real-time risk assessments. Where do you see the biggest impact of these technologies, and how should organisations embrace them responsibly?



An increasing number of compliance firms are using AI (or often, more accurately, ML and NLP) to extract risk signals from large amounts of data.

However, for every great marketing ad shouting the value of 'AI,' it's important to remember that AI can produce incorrect outputs if the underlying models aren't well-trained or validated. I've lost count of the number of times I've asked an AI system questions and received results I knew were wrong, so be careful.

Use AI to accelerate data analysis, but make sure there's a human layer to verify critical risk findings.



As regulation tightens, simply skimming headlines won't cut it. Organisations need a comprehensive approach to spot early warnings in global media—not just the mainstream outlets.

Toby Cook,
CSO @ Opoint

**Got Compliance Questions?
Schedule a Call with Toby**



Lessons from Real-World Compliance Failures

Even with strong programs, lapses can happen, and regulators are cracking down harder than ever. Recent enforcement actions carry strategic lessons for compliance officers:

- **Bigger fines, bigger headlines:** Authorities like the U.K. Financial Conduct Authority (FCA) and the U.S. Department of Justice (DOJ) have shown little leniency toward institutions that fail in compliance.

Multi-million and even billion-dollar fines are now routine, and every penalty comes with damaging press coverage. The era of quietly settling issues is over; enforcement today often means front-page news.

- **Accountability and culture:** Many recent cases also underscore that regulators will hold not just institutions, but individuals and leadership accountable for compliance failings. This has driven home the need for a top-down culture of compliance.

When leaders prioritise growth over compliance, the consequences can include career-ending enforcement actions. Conversely, a strong compliance culture can catch issues before regulators do.





Case in Point: Notable Compliance Failures

Several high-profile cases from the past few years highlight how things can go wrong and the importance of the measures discussed in this playbook.

TD Bank's Compliance Collapse



In October 2024, TD Bank pleaded guilty to violations of federal anti-money laundering laws and the Bank Secrecy Act.

The bank admitted to “long-term, pervasive and systemic deficiencies” in its AML controls. The result was a record-breaking penalty of over \$3 billion in total fines. Regulators found that between 2014 and 2023, TD failed to monitor approximately \$18.3 trillion in customer transactions, roughly 92% of its transaction volume went unmonitored.

This lapse enabled at least three money-laundering networks to funnel more than \$670 million in illicit funds through the bank. Officials described TD as having created a “convenient environment” for bad actors.

The fallout was severe: the CEO and global AML officer resigned, several executives were dismissed, and U.S. regulators imposed an asset cap that restricts TD's growth until it fixes its compliance issues.

Lesson:

Comprehensive due diligence and ongoing monitoring of correspondent and cross-border relationships are essential.

Even large, well-established banks must continuously invest in compliance expertise and technology. What seems like a routine business relationship can hide enormous risks if not properly vetted and watched.



Nordea Bank's Due Diligence Shortcomings



In 2024, Nordea Bank (the largest Nordic bank) agreed to a \$35 million settlement with New York State's Department of Financial Services over significant AML compliance failures.

Regulators found Nordea's due diligence on high-risk correspondent banking was severely lacking. In fact, between 2008 and 2019, billions of dollars in high-risk, suspect transactions flowed through Nordea, some linked to infamous schemes exposed by the Panama Papers. The bank had missed obvious red flags in its Baltic and other operations, even acknowledging internally that its oversight faced a "critical" risk of failure.

Nordea's chief compliance officer admitted the bank had historically "underestimated the complexity of preventing financial crime and the resources needed" for compliance.

Lesson:

Comprehensive due diligence and ongoing monitoring of correspondent and cross-border relationships are essential. Even large, well-established banks must continuously invest in compliance expertise and technology.

What seems like a routine business relationship can hide enormous risks if not properly vetted and watched.





ABN AMRO's Monitoring Failures



In 2021, Dutch bank ABN AMRO was fined €480 million by the Netherlands Public Prosecution Service for serious shortcomings in its AML processes. Prosecutors found that for years, the bank failed to adequately identify and report suspicious transactions, allowing certain clients to abuse accounts for criminal activities unabated.

ABN AMRO had been accused of ignoring obvious signs of money laundering, not exiting suspicious clients and not alerting authorities as required. The investigation even led to the implication of former executives for their role in oversight failures.

Lesson:

Even in a well-regulated environment like the Netherlands, a lapse in continuous monitoring and client review can result in criminals exploiting the financial system.

A culture of compliance, where employees feel responsible for flagging and acting on unusual activity, might have prevented such long-running failings. This case also shows regulators will not hesitate to impose huge penalties and even pursue individual accountability when systemic failures occur.

Across these cases, common threads emerge.

Underestimating compliance (whether by under-resourcing it or treating it as a formality) can lead to massive fines and operational restrictions. High-risk areas like correspondent banking and cross-border flows need extra attention and perpetual risk assessment.

Globally, regulators are coordinating and escalating their enforcement, but no major institution is out of reach. For compliance professionals, these cautionary tales underscore the importance of proactive monitoring, strong internal escalation of issues, and cultivating an organisational culture that supports compliance at every level.



How Opoint Helps You Stay Compliant

Implementing the strategies in this playbook can be challenging without the right tools. This is where compliance data platforms like Opoint come into play, acting as force multipliers for your team. Opoint's solutions are designed to address many of the daily hurdles compliance professionals face.

Global Coverage

Opoint provides access to 235,000+ sources in over 150 languages, covering more than 220 jurisdictions. This extensive reach is ideal for comprehensive adverse media screening – you won't miss that critical article in a small local outlet halfway around the world.

Clean, Structured Data

Opoint's feeds come in a clean, machine-readable format, stripped of ads or irrelevant clutter. Each article is enriched with metadata. This structure means the data captured is directly usable for automated processing and easy searching, reducing noise and focusing on what truly matters.

End-to-End Integration

The data is designed to plug into your existing compliance and risk infrastructure. Whether you use a third-party case management system or an in-house dashboard, Opoint's API and data format make integration straightforward. This plug-and-play approach ensures you can incorporate global news monitoring into your workflows with minimal IT hassle.

Metadata Enrichment

Each piece of content comes tagged with useful metadata like location, language, and names of companies or individuals (using identifiers such as LEIs, FIGIs, and PermIDs). This enrichment streamlines your processing – you can filter or search the feed by these tags to quickly hone in on risk-relevant content (for example, all news related to a specific client across all languages).



Future-Proof Your Compliance Strategy

Regulatory fines, public scrutiny, and reputational fallout are all on the rise. Compliance is not a static checklist but a dynamic function that must continuously adapt.

To future-proof your strategy, focus on integrating perpetual monitoring into your processes, managing and securing data responsibly, and building a strong adverse media screening framework. By doing so, you'll be well-positioned to sidestep potential crises before they strike.

The organisations that succeed in the coming years will be those that anticipate risks rather than merely react to them.

The world of compliance is ever-changing.

New regulations, technologies, and threats are emerging all the time. To minimise risk, you need real-time coverage of information, robust internal controls, and seamless data processing.

Incorporating non-English sources into your monitoring greatly amplifies your protective net, ensuring you aren't blindsided by events in far-flung locales.

At the same time, maintaining a human touch – expert analysis, ethical judgment, and cross-team collaboration – is what turns raw data into an effective compliance shield.

Invitation to Continue the Conversation



Staying ahead of global risks is an ongoing journey.

We encourage you to take the insights from this playbook and evaluate your own compliance framework. Identify one or two areas where a data-driven upgrade could make a big difference, and start there.

And if you're curious how a solution like Opoint can supercharge these efforts, consider [booking a demo](#) to see it firsthand.

We're here to help compliance professionals, like you, bolster your defenses, protect personal information, and manage third-party risks in your supply chain. In the realm of compliance, knowledge – and speed – are everything.



Key Takeaways

- **Adverse Media Screening:** A vital tool for spotting early red flags in news coverage (in any language) about clients, partners, or employees.
It moves compliance beyond ticking boxes, catching issues that pure transaction monitoring might miss.
- **Real-Time Monitoring:** Perpetual, real-time surveillance of transactions and news minimises blind spots and reduces manual workload. This lets your team focus on high-level analysis and decision-making, rather than data gathering.
- **Global, Non-English Sources:** Tapping into news and data from around the world is a hidden superpower in heading off financial crime and reputational pitfalls.
Many risks manifest abroad or in foreign languages first – don't let language be a barrier to your awareness.
- **Managing Third-Party Risks:** Ensure that not just your company but also your third-party vendors and partners maintain strong compliance and data security practices.
Your compliance framework should extend through your entire business network, because weak links can expose you to just as much risk.
- **Proactive Compliance Culture:** Foster an environment where ongoing learning is encouraged, and new technologies (from machine learning to advanced analytics) are embraced judiciously.
A culture that values compliance will support swift adoption of better tools and practices, keeping the organisation ahead of the curve.

A robust compliance programme doesn't just protect you from fines, it preserves your brand's reputation and assures clients and stakeholders that their trust is well-placed. By strengthening your data-driven practices today, you equip your organisation to navigate the uncertainties of tomorrow.

If you're ready to see how Opoint's solutions can fit into your broader compliance ecosystem, book a demo and discover what multilingual, real-time data can do for you.

Your journey to smarter compliance starts now